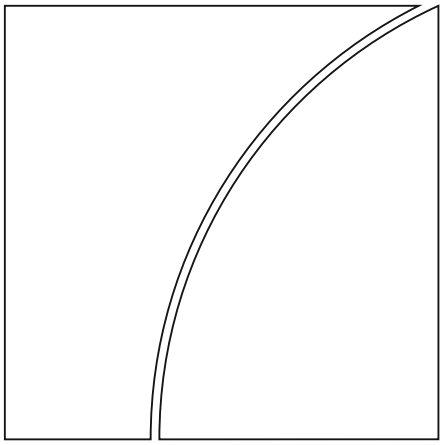
Basel Committee
on Banking Supervision



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

December 2013

BANK FOR INTERNATIONAL SETTLEMENTS

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

ISBN 92-9131-978-3 (print)

ISBN 92-9197-978-3 (online)

Contents

Executive summary

Background

1. The *Principles for effective risk data aggregation and risk reporting* (the Principles) were issued by the Basel Committee on Banking Supervision (the Basel Committee) in January 2013.[1] The Principles aim to strengthen risk data aggregation and risk reporting practices at banks to improve risk management practices. In addition, improving banks' ability to rapidly provide comprehensive risk data by legal entity and business line will enhance banks' decision-making processes and improve their resolvability.

2. The Principles are initially addressed to systemically important banks (SIBs) and apply not only at the group level but also to all material business units or entities within the group. National supervisors may nevertheless choose to apply the Principles to a wider range of banks. The Basel Committee and the Financial Stability Board (FSB) expect banks identified as global systemically important banks (G-SIBs) to comply with the Principles by 1 January 2016.[2] In addition, the Basel Committee strongly suggests that national supervisors also apply the Principles to banks identified as domestic systemically important banks (D-SIBs) three years after their designation as such by their national supervisors.

3. The Basel Committee and national supervisors agreed to monitor and assess banks' progress through the Basel Committee's Supervision and Implementation Group (SIG), which will share its findings with the FSB at least annually from the end of 2013. To facilitate consistent and effective implementation of the Principles among G-SIBs, the SIG decided to use a coordinated approach for national supervisors to monitor and assess banks' progress until 2016. The first step of this coordinated approach was to implement a "stocktaking" self-assessment questionnaire completed by G-SIBs during 2013.

G-SIBs' self-assessments

4. The Basel Committee's Working Group on SIB Supervision (WGSS) developed the questionnaire (87 questions/requirements for 11 principles), analysed the results and set out several recommendations for 2014 to ensure that banks are able to meet the 2016 deadline. National supervisors and the WGSS understand that many banks found it challenging to complete the questionnaire and made significant efforts in collecting inputs, in part because the questionnaire was circulated shortly after issuance of the Principles.

5. The WGSS is confident that the questionnaire results broadly reflect the current state of implementation based on members' knowledge of participating banks. Nevertheless, several caveats apply to the results. For example, the outcomes in this paper are based on self-assessments by banks that were conducted on a best efforts basis. Moreover, the ratings assigned as part of the self-assessment process (ranging in compliance status from 4 (best) to 1 (worst)) were defined broadly and may therefore have been interpreted more or less conservatively across banks. In addition, although national supervisors reviewed responses and discussed them with banks in their jurisdictions, they were

[1] The Principles can be found at www.bis.org/press/p130109.htm.

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

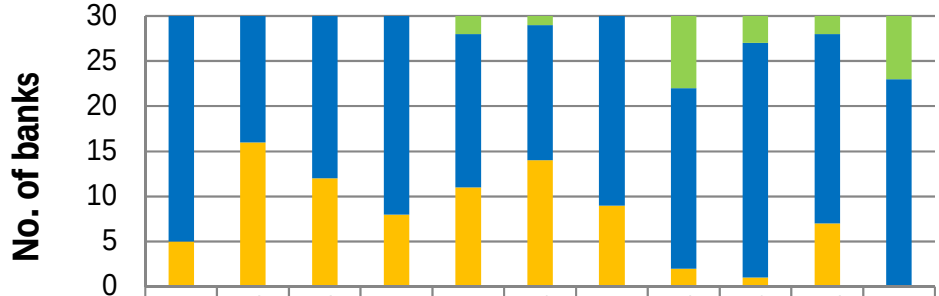
not asked to validate the accuracy of the ratings or comments, nor did they assess the potential differences in the level of rigor applied by each bank or differences in home/host supervisory approaches. The results may, therefore, be best understood as providing a snapshot of banks' overall preparedness to comply with the Principles, as well as the relative challenges faced.

6. Thirty G-SIBs identified in 2011 and 2012 (Annex 1) responded to the questionnaire. Banks' responses were anonymised and forwarded to the Basel Committee Secretariat by national supervisors. The WGSS analysis team and the Secretariat analysed those responses on the condition that the information be kept strictly confidential. Through their responses, banks demonstrated that they understand the importance of the Principles and are committed to enhancing their risk data aggregation and risk reporting capabilities. Although at this initial stage each G-SIB's reported compliance status with each Principle still varies, supervisors are committed to ensuring their G-SIBs will fully comply with the Principles by the deadline. The key findings below reflect the banks' and supervisors' views.

7. As depicted in the chart below, the average ratings of Principles 1 to 11 ranged from 2.5 to 3.2. The average rating of all 11 principles was 2.8, which indicates that banks' average reported compliance status stands between largely compliant and materially non-compliant. It is noted that the three principles with the lowest reported compliance were Principle 2 (data architecture/IT infrastructure), Principle 6 (adaptability) and Principle 3 (accuracy/integrity); nearly half of banks reported material non-compliance on these principles. Indeed, many banks are facing difficulties in establishing strong data aggregation governance, architecture and processes, which are the initial stage of implementation. Instead they resort to extensive manual workarounds which are likely to impair risk data aggregation and reporting.

8. The principles for which banks reported the highest compliance pertained to reporting: Principles 11 (report distribution), 8 (comprehensiveness) and 9 (clarity/usefulness). Broadly speaking, reporting principles had better scores than governance/infrastructure and data aggregation principles. For example, as depicted below, compliance with Principle 2 (data architecture/IT infrastructure) was rated lowest while Principle 11 (report distribution) was rated highest. This result is difficult to interpret because the Principles state that governance/infrastructure principles are "preconditions to ensure compliance with the other [p]rinciples".

Self assessment ratings by Principles



	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11
Fully compliant	0	0	0	0	2	1	0	8	3	2	7
Largely compliant	25	14	18	22	17	15	21	20	26	21	23
Materially non-compliant	5	16	12	8	11	14	9	2	1	7	0
Non-compliant	0	0	0	0	0	0	0	0	0	0	0
Average rating	2.8	2.5	2.6	2.7	2.7	2.6	2.7	3.2	3.1	2.8	3.2
	Governance/ infrastructure		Risk data aggregation capabilities					Risk reporting practices			

See Annex 2 for the list of 11 Principles and 87 requirements.

9. Looking at individual banks, nearly half reported full compliance with at least one principle, although this was largely limited to one principle, while approximately 20% of banks reported material non-compliance with nearly half of the 11 principles.

10. All banks indicated that they are making efforts towards closing all significant gaps by the 2016 deadline, but in some cases the expected compliance dates set by some banks seem to be overly optimistic. More importantly, 10 banks, 33% of the population, mentioned that they currently expect to not fully comply with at least one principle by the deadline. Some of these banks noted that the reason is large, ongoing, multi-year, in-flight IT and data-related projects.

11. Key weaknesses have been identified through this exercise:

Overarching weaknesses

(a) In many case banks' self-assessment scope was limited to the group level and did not take into account each material business unit or entity within the group. Supervisors agree that these Principles apply not only at the group level, but also to all material business units or entities within the group. Second, when rating themselves on risk reporting Principles, a number of banks only focused on the quality of risk reports to senior management and the boards (not including middle management). Third, there is evidence that many banks assessed only a few types of risk, such as credit risk and market risk, while not comprehensively covering other types of risk, such as liquidity risk, operational risk and other risks. Fourth, very few banks offered insights into their definitions of materiality or tolerance level for manual versus automated processes for risk data aggregation and reporting. Some banks may have used those definitions to justify higher compliance ratings than may be warranted.

(b) These self-assessment scope limitations raise concerns that the ratings chosen by banks may not accurately reflect their compliance status, covering all material group entities, all levels of management and all types of material risk. Therefore, banks need to ensure that their implementation scope appropriately reflects the intended scope of the Principles.

Governance and infrastructure

(c) In order to fully comply with the Principles, banks need to significantly upgrade their risk IT systems and governance arrangements. Banks need to have in place: (i) formal and documented risk data aggregation frameworks; (ii) comprehensive data dictionaries that are used consistently by all group entities; (iii) a comprehensive policy governing data quality controls; and (iv) controls through the life cycle of data. Banks also need to ensure that the role of the "data owner" is clearly documented and to set out accountability for risk data quality. In order to effectively support risk data aggregation and risk reporting practices, banks also must resolve the significant limitations currently affecting their risk IT systems. Banks that have not yet established their plans for independent validation of their data aggregation and reporting must make concrete efforts towards these goals.

Risk data aggregation capabilities

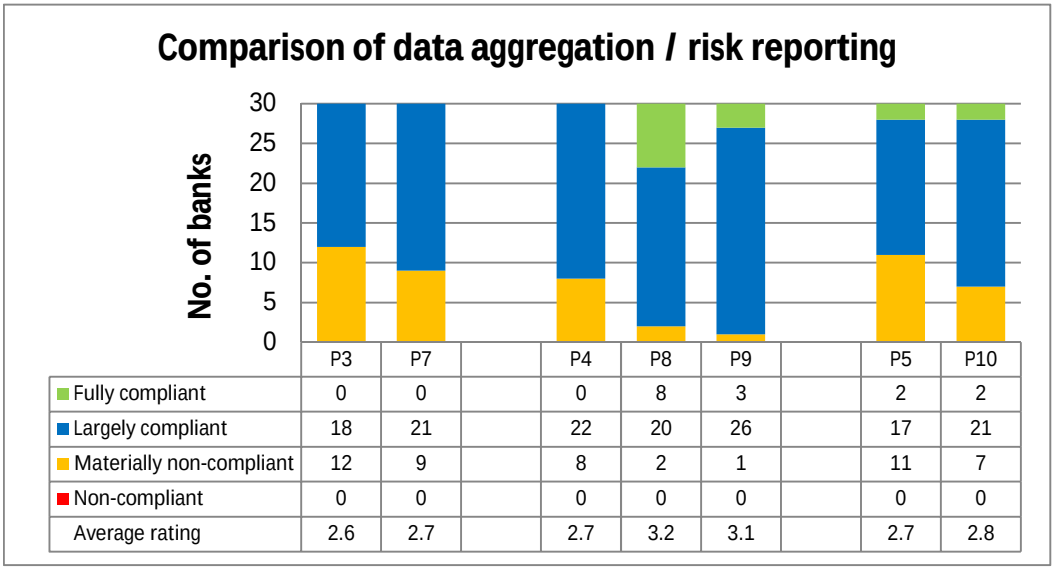
(d) Banks also have to make significant efforts to improve their risk data accuracy, completeness, timeliness and adaptability. Banks often rely on manual processes, which impair their ability to ensure accuracy and timeliness of data, particularly in stress situations. These challenges affected banks' risk management capabilities during the recent financial crisis. The banks also need to ensure that the data quality checks supporting their risk data are as robust as those supporting their accounting data. Adaptability was one of the lowest-rated principles in this

category, and banks must ensure that they can generate relevant data on a timely basis to meet evolving internal and external risk reporting requirements. Banks need to have in place: (i) an appropriate balance between automated and manual systems that allows rapid aggregation of data, even in stress times; (ii) documentation of timely risk data aggregation processes; (iii) a data definition consistent across the organisation; and (iv) customisation of data to users' needs.

Risk reporting practices

(e) A number of banks, when rating individual principles, failed to take into account the interdependencies between the three areas of the Principles (governance and infrastructure, data aggregation, and risk reporting). In particular, within the data aggregation and risk reporting categories there are principles that closely align, with the intention of ensuring that compliance with the risk reporting principles is achieved through fully compliant data aggregation practices.

(f) As shown below, banks generally assigned themselves higher ratings on the risk reporting principles than they did on the corresponding data aggregation principles. This includes a few banks that rated themselves fully compliant on Principle 8 (comprehensiveness) and materially non-compliant on one or more data aggregation principles. This raises a question as to how reliable and useful risk reports can be when the data within these reports and the processes to produce them have significant shortcomings. In this regard, banks may have overstated their actual level of compliance with risk reporting principles with regard to: (i) ability to rapidly collect, analyse and report on risk exposures due to overreliance on manual processes; (ii) frequency of ad hoc stress/scenario reporting; and (iii) formal procedures for rapid collection and analysis of risk data and timely dissemination of reports. In addition, banks rated themselves relatively low on: (i) automated and manual edit and reasonableness checks; (ii) use of an integrated procedure to identify data errors; and (iii) inventory and classification of risk data items.



	P3	P7		P4	P8	P9		P5	P10
Fully compliant	0	0		0	8	3		2	2
Largely compliant	18	21		22	20	26		17	21
Materially non-compliant	12	9		8	2	1		11	7
Non-compliant	0	0		0	0	0		0	0
Average rating	2.6	2.7		2.7	3.2	3.1		2.7	2.8

Definition of Principles: P3 = accuracy and integrity; P7 = accuracy; P4 = completeness; P8 = comprehensiveness; P9 = clarity and usefulness; P5 = timeliness; P10 = frequency.

Other large banks' self-assessments

12. In addition to G-SIBs, the Basel Committee indicated that national supervisors could voluntarily include other large banks in the exercise. Consequently, six other large banks in four jurisdictions participated in the questionnaire. In most cases, these banks reported that they were largely compliant with the 11 Principles. None of them rated themselves as fully compliant or non-compliant with any of the Principles. All but one of the banks expects to comply with the Principles by January 2016, with time frames of June 2014 to January 2016. With regard to the comparison between other large banks and G-SIBs, in general, other large banks had slightly wider compliance gaps than G-SIBs across all principles (although the small size of the sample calls for caution in drawing comparisons).

Supervisory plans and next steps

13. According to the stocktaking questionnaire for national supervisors, all participating supervisory authorities are committed to achieving full compliance by G-SIBs with the Principles by 1 January 2016. The stocktaking exercise shows that supervisory authorities are already doing meaningful work in overseeing the Principles. Supervisors review relevant aspects of banks' risk data aggregation and reporting frameworks in their existing supervisory programmes and through their assessment of related banking areas. In addition, supervisory authorities have a broad range of tools and remedial actions to enforce the Principles and have the expertise/resources to monitor banks' progress towards implementation. Based on this exercise, it is recommended that supervisory authorities consider enhancing their efforts to: (i) fully integrate the Principles in a comprehensive way within their supervisory programmes; (ii) test banks' capabilities to aggregate and produce reports in stress/crisis situations, including resolution; (iii) conduct thematic reviews; and (iv) develop concrete supervisory plans or other supervisory tools for 2014 and 2015.

14. With regard to next steps, in order to ensure that G-SIBs will fully comply with the Principles by the deadline, national supervisors will investigate the root causes of non-compliance, and use supervisory tools or appropriate discretionary measures depending on banks' situations. National supervisors and the WGSS should ensure that in 2014 banks move further towards implementation, bearing in mind that if they are to produce high-quality risk data and risk reports, they need to build up strong risk data governance and architecture and robust aggregation capabilities. As relevant, that work will be coordinated by the WGSS with the implementation of other G-SIB/D-SIB standards under the Regulatory Consistency Assessment Programme (RCAP). In the two remaining years before entry into force, the WGSS is contemplating the following steps:

(a) Conduct a self-assessment survey of banks in a reduced form and a thematic review of the requirements with lowest scores

(b) National supervisors' review of banks' self-assessments

(c) Stress tests to require banks to complete a risk data aggregation template within a limited time

1. Introduction

The *Principles for effective risk data aggregation and risk reporting* were issued by the Basel Committee in January 2013. The Principles aim to strengthen risk data aggregation and risk reporting practices at banks to improve risk management practices. In addition, improving banks' ability to rapidly provide comprehensive risk data by legal entity and business line will enhance banks' decision-making processes and improve their resolvability.

The Principles are initially addressed to SIBs and apply not only at the group level but also to all material business units or entities within the group. National supervisors may nevertheless choose to apply the Principles to a wider range of banks. The Basel Committee and the FSB expect banks identified as G-SIBs to comply with the Principles by 1 January 2016. To meet this deadline, G-SIBs are expected to start making progress towards effectively implementing the Principles from early 2013. In addition, the Basel Committee strongly suggests that national supervisors also apply the Principles to banks identified as D-SIBs three years after their designation as such by their national supervisors.

The Basel Committee and national supervisors agreed to monitor and assess banks' progress through the Basel Committee's SIG, which will share its findings with the FSB at least annually from the end of 2013. To facilitate consistent and effective implementation of the Principles among G-SIBs, the SIG decided to use a coordinated approach for national supervisors to monitor and assess banks' progress until 2016. The first step of this coordinated approach was to implement a "stocktaking" self-assessment questionnaire completed by G-SIBs during 2013.

The Basel Committee's Working Group on SIB Supervision developed the questionnaire, analysed the results, and set out several recommendations for 2014 to ensure that banks are able to meet the 2016 time frame. Thirty G-SIBs identified in 2011 and 2012 and six other large banks participated in the questionnaire. Banks' responses were anonymised and forwarded to the Basel Committee Secretariat by national supervisors. The WGSS analysis team and the Secretariat analysed those responses on the condition that the information be kept strictly confidential.

2. Bank questionnaire – objectives, scope and process

2.1 Objectives

The objective of the questionnaire was to establish how each G-SIB views its current level of compliance with Principles 1 through 11. The stocktake enables the supervisory authorities to monitor and promote progress towards full compliance by the 2016 deadline, and to help identify and remediate any implementation issues. The questionnaire is a useful tool for banks to familiarise themselves with the Principles and should help them progress towards meeting the 2016 deadline.

2.2 Scope

The questionnaire included 87 detailed requirements that must be met to comply with all of the Principles (Annex 2). The Principles were divided into three areas:

- Governance and infrastructure
- Risk data aggregation capabilities
- Risk reporting practices

These areas are interrelated. High-quality risk reports rely on strong risk data aggregation capabilities, and sound governance and infrastructure ensures adequate information flow within an organisation.

2.3 Self-assessment rating

In the questionnaire, banks were requested to rate, on a scale from 1 to 4, their current level of compliance with 11 Principles and 87 specific requirements under the Principles. The four ratings were defined as follows:

1. The principle/requirement has not yet been implemented.
2. The principle/requirement is materially non-compliant and significant actions are needed in order to progress further or achieve full compliance with the principle/requirement.
3. The principle/requirement is largely compliant with and only minor actions are needed to fully comply with the principle/requirement.
4. The principle/requirement is fully compliant with and the objective of the principle/requirement is fully achieved with the existing architecture and processes.

It was anticipated that if compliance with any requirement under a principle was rated below 4, then the general level of compliance with the principle would also be rated below 4. It was also anticipated that the interdependencies among the three categories of principles would be factored into the ratings, such that the data aggregation and risk reporting principles would not be rated as fully compliant until the underlying governance and infrastructure principles were rated as fully compliant. Likewise, it was anticipated that the risk reporting principles would not be rated as fully compliant until the corresponding data aggregation principles were rated as fully compliant.

2.4 Process

National supervisors issued letters to the 30 G-SIBs and six other large banks in March 2013, asking them to complete the questionnaire by no later than 1 July 2013. Banks self-assessed their current level of compliance with each principle. National supervisors reviewed and analysed the banks' responses via follow-up meetings or conference calls and provided the WGSS with a written assessment of their respective banks' responses. During these interactions, banks and national supervisors discussed:

- The process followed to complete the questionnaire
- Any areas where national supervisors thought that ratings might not be accurate
- The bank's strategy to comply with the Principles

The observations, recommendations, and conclusions in this paper are based on self-assessments completed by the participating banks. National supervisors were not asked to validate the accuracy of the ratings or comments, nor did they assess the potential differences in the level of rigor applied by each bank or differences in home/host supervisory approaches.

3. G-SIBs' practices and approaches

This section summarises the findings from the 30 G-SIBs' responses to the questionnaire, showing their level of reported compliance with Principles 1–11. The outline of each subsection is as follows:

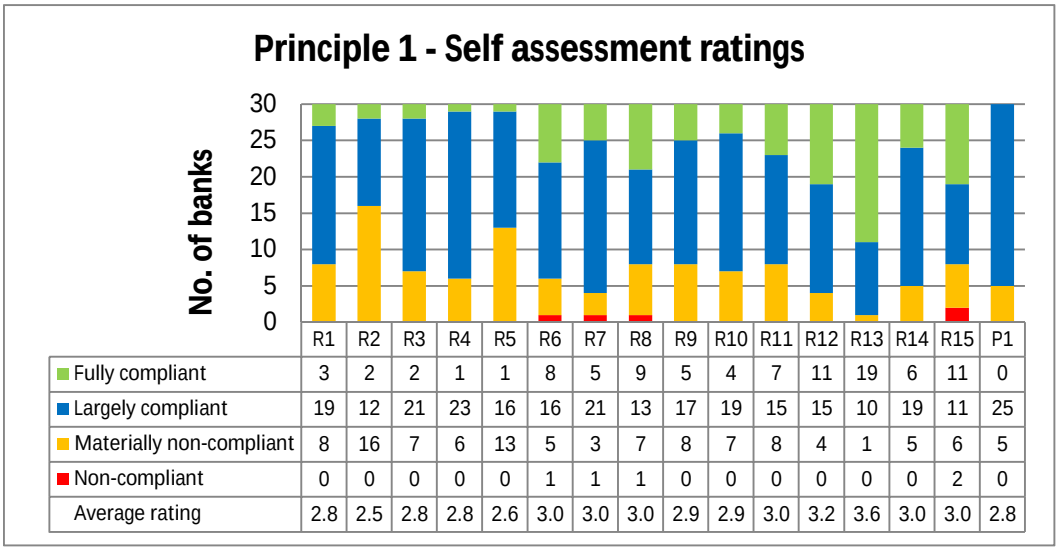
(i) Text of each Principle

(ii) Bar chart displaying the ratings distribution for each Principle (last bar to the right) and the underlying requirements for the Principle. To assist with the interpretation of the results, an average rating was calculated for each Principle and each requirement. A table containing these average ratings is also available in Annexes 3 and 4.

(iii) High-level summary of the results – overall ratings' frequency/average, highest/lowest average ratings among underlying requirements, general timeline for full compliance and main challenges.

3.1 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.



	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	P1
Fully compliant	3	2	2	1	1	8	5	9	5	4	7	11	19	6	11	0
Largely compliant	19	12	21	23	16	16	21	13	17	19	15	15	10	19	11	25
Materially non-compliant	8	16	7	6	13	5	3	7	8	7	8	4	1	5	6	5
Non-compliant	0	0	0	0	0	1	1	1	0	0	0	0	0	0	2	0
Average rating	2.8	2.5	2.8	2.8	2.6	3.0	3.0	3.0	2.9	2.9	3.0	3.2	3.6	3.0	3.0	2.8

As shown in the P1 bar, 83% of banks rated themselves as largely compliant with Principle 1 and 17% rated themselves materially non-compliant. The average rating for this principle was 2.8.

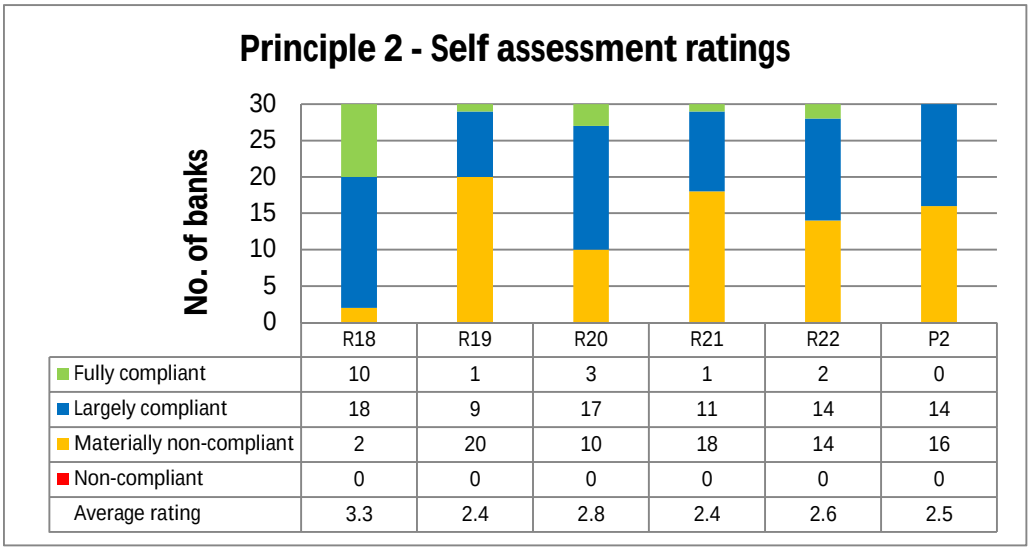
While no banks rated themselves as fully compliant, 90% indicated that they expected to comply by the January 2016 deadline, with expected compliance dates that ranged from December 2014 to January 2016. One of the three banks with a time frame beyond the deadline expected to comply by June 2016.

Fifteen requirements supported the assessment of this principle. The average rating assigned to each requirement ranged from 2.5 to 3.6. As shown in the chart, R2 (approval of the framework and resources deployed) and R5 (full documentation and validation) received 16 and 13 materially non-compliant ratings, respectively, which represent the two lowest-rated requirements under this Principle. R2 was the fifth lowest among all 87 requirements. Surprisingly, R15 (board's awareness of implementation and ongoing compliance) had two non-compliant ratings. The boards of these two banks should be aware of their implementation of the Principles. R6 (independent validation by qualified staff), R7 (consideration as part of any new initiatives), and R8 (assessment of the data aggregation process in case of acquisitions) had one non-compliant rating each.

The main challenges and issues regarding governance arrangements include:

- Establishment of formal high-level review/approval of a comprehensive group risk data aggregation and risk reporting framework, including service-level standards for risk data-related processes (also for outsourced processes), policies on data confidentiality and integrity, and risk management policies (related to R1, R2 and R4).
- Full documentation of risk data aggregation capabilities and risk reporting practices; establishment of high internal standards for independent validation; and full integration of validation into the broader "second line of defence" risk management programme (related to R5).
- Identification, assessment and management of data quality risk (related to R3).

Principle 2 – Data architecture and IT infrastructure – A bank should design, build and maintain data architecture and IT infrastructure which fully supports its risk data aggregation capabilities and risk reporting practices not only in normal times but also during times of stress or crisis, while still meeting the other Principles.



	R18	R19	R20	R21	R22	P2
Fully compliant	10	1	3	1	2	0
Largely compliant	18	9	17	11	14	14
Materially non-compliant	2	20	10	18	14	16
Non-compliant	0	0	0	0	0	0
Average rating	3.3	2.4	2.8	2.4	2.6	2.5

As shown in the P2 bar, the population was nearly evenly split between largely compliant and materially non-compliant ratings. The average rating for this Principle was 2.5, the lowest rating among the 11 Principles. Thus, data architecture and IT infrastructure seem to be the toughest and most critical challenge for banks.

While no banks rated themselves fully compliant, 73% expected to comply by the January 2016 deadline, with expected compliance dates that ranged from June 2015 to January 2016. One of the remaining eight banks (27%) expected to achieve compliance in December 2018, three years after the deadline. Many of the "post-2016" banks referenced pending large-scale IT and data projects that will extend past the deadline, while a few banks indicated that the degree of compliance will depend on the intended scope of the Principles.

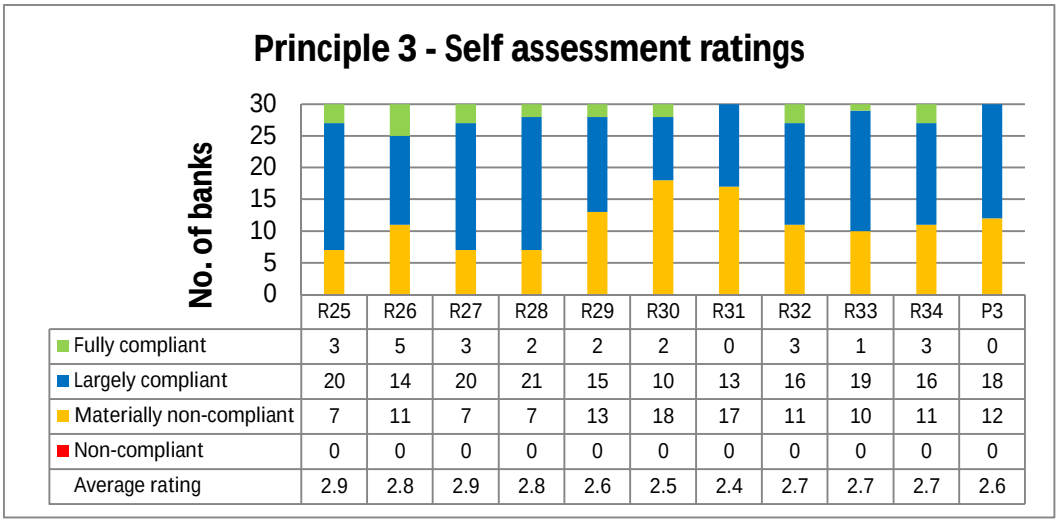
Five requirements supported the assessment of this Principle. The average rating assigned to each requirement ranged from 2.4 to 3.3. As shown in the chart, R19 (data taxonomies) and R21 (role of business owner) received 20 and 18 materially non-compliant ratings, respectively, making them the two lowest-rated of all 87 requirements. In addition, R22 (adequate controls through the life cycle of data) had a relatively low score of 2.6 compared with other requirements.

The main challenges and issues regarding data architecture and IT infrastructure include:

- Incomplete group-wide centralisation/standardisation of integrated data taxonomies and architecture (dictionaries, definitions and metadata). It is often unclear whether stated convergence plans are at design, pilot or live stage (related to R19).
- Accountability for data control responsibilities throughout the data life cycle are often opaque; demarcation of duties among business owner, IT and risk management is unclear or uneven across risk types, legal entities and portfolios. Most G-SIBs were not in a position to attest that they had high-quality assurance standards covering the entire data life cycle (related to R21 and R22).
- Completion and rollout of "risk data" modules within business continuity plans (impact simulation, target recovery indicators, process updates as needed). It is often unclear whether banks are at design, pilot or live stage (related to R18).

3.2. Risk data aggregation capabilities

Principle 3 – Accuracy and Integrity – A bank should be able to generate accurate and reliable risk data to meet normal and stress/crisis reporting accuracy requirements. Data should be aggregated on a largely automated basis so as to minimise the probability of errors.



	R25	R26	R27	R28	R29	R30	R31	R32	R33	R34	P3
Fully compliant	3	5	3	2	2	2	0	3	1	3	0
Largely compliant	20	14	20	21	15	10	13	16	19	16	18
Materially non-compliant	7	11	7	7	13	18	17	11	10	11	12
Non-compliant	0	0	0	0	0	0	0	0	0	0	0
Average rating	2.9	2.8	2.9	2.8	2.6	2.5	2.4	2.7	2.7	2.7	2.6

As shown in the P3 bar, the population was largely evenly split between largely compliant and materially non-compliant ratings. The average rating for this Principle was 2.6, which was the third lowest score among the 11 principles.

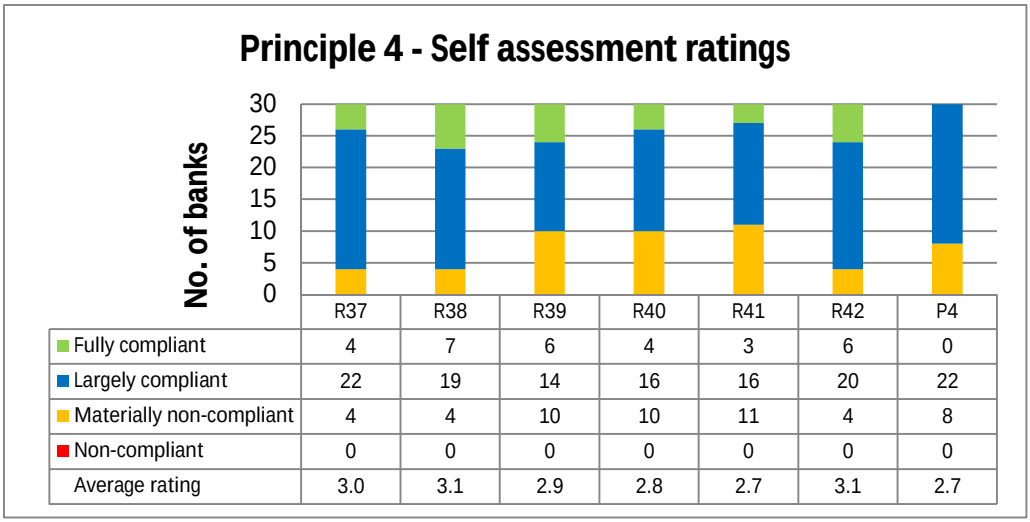
While no banks rated themselves as fully compliant, 83% of banks expected to comply by the January 2016 deadline, with expected compliance dates that ranged from July 2015 to January 2016. One of the remaining five banks (17%) had an estimated compliance date of December 2017, two years after the deadline. Four banks indicated that they would not be able to fully comply due to in-flight multi-year IT infrastructure and data aggregation projects that were not scheduled to complete by January 2016.

Ten requirements supported the assessment of this Principle. The average rating assigned to each requirement ranged from 2.4 to 2.9. As shown in the chart, R30 (balance between automated and manual systems) and R31 (documentation of risk data aggregation processes) received 18 and 17 materially non-compliant ratings, respectively, making them the third and fourth lowest of all 87 requirements. In addition, R29 (dictionary) had a relatively low score of 2.6.

The main challenges and issues regarding generating accurate risk data to meet normal and stress reporting requirements include:

- Inadequate IT systems, including both source data systems and aggregation engines, that are scattered across many business units or entities and cannot fully support accurate generation of risk data on a timely basis (related to R28 and R31–33).
- A level of dependency on manual processes that poses a challenge to accurate and timely risk data aggregation (related to R30).
- A large number of banks do not have consistent processes and data terminologies across their groups because of decentralised business models and a lack of group-wide policies and procedures (related to R29).

Principle 4 – Completeness – A bank should be able to capture and aggregate all material risk data across the banking group. Data should be available by business line, legal entity, asset type, industry, region and other groupings, as relevant for the risk in question, that permit identifying and reporting risk exposures, concentrations and emerging risks.



	R37	R38	R39	R40	R41	R42	P4
Fully compliant	4	7	6	4	3	6	0
Largely compliant	22	19	14	16	16	20	22
Materially non-compliant	4	4	10	10	11	4	8
Non-compliant	0	0	0	0	0	0	0
Average rating	3.0	3.1	2.9	2.8	2.7	3.1	2.7

As shown in the P4 bar, 73% of banks indicated that they were largely compliant, while 27% indicated that they were materially non-compliant. The average rating for this Principle was 2.7.

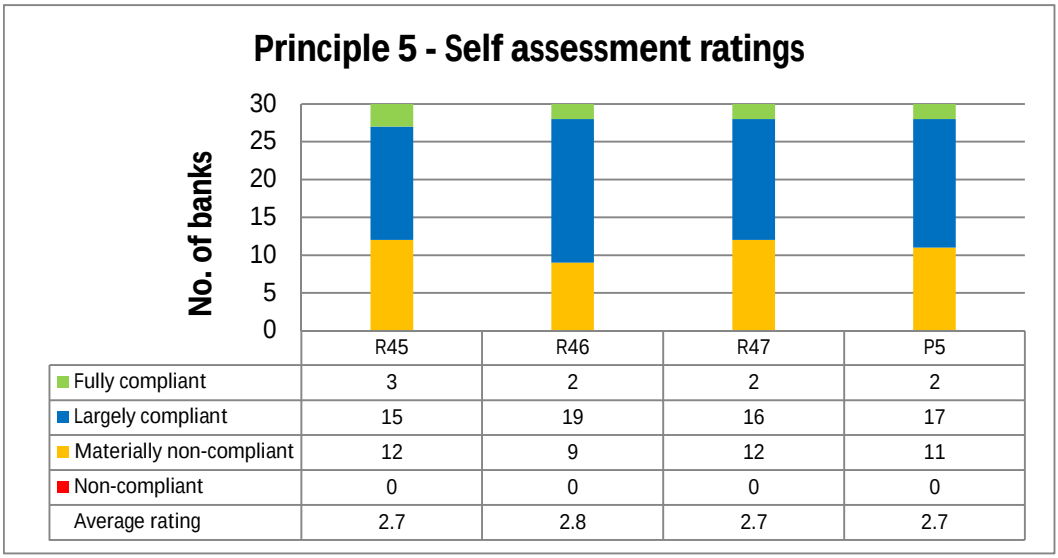
While no banks rated themselves as fully compliant, 80% of banks expected to comply by the January 2016 deadline, with expected compliance dates that ranged from December 2014 to January 2016. Three of the remaining six banks (20%) had estimated compliance dates of December 2016 or January 2017, one year after the deadline. Four banks indicated that they would not be able to fully comply by this deadline due to in-flight multi-year data-related projects.

Six requirements supported the assessment of this Principle. The average rating assigned to each requirement ranged from 2.7 to 3.1. As shown in the chart, R41 (exceptions properly identified and explained), R39 (documentation of approaches to aggregate exposures) and R40 (measurement and monitoring of all material risk data) received 11, 10 and 10 materially non-compliant ratings, respectively, which represented the three lowest-rated requirements under this Principle.

The main challenges and issues regarding completeness across the banking group include:

- Lack of formally defined and documented tolerance levels to ascertain material exceptions (related to R41).
- Insufficient monitoring processes across the group and/or across all material risk types (related to R40).
- Inadequate or insufficient documentation available to the board and senior management regarding the bank's approach to risk data aggregation (related to R39).

Principle 5 – Timeliness – A bank should be able to generate aggregate and up-to-date risk data in a timely manner while also meeting the principles relating to accuracy and integrity, completeness and adaptability. The precise timing will depend upon the nature and potential volatility of the risk being measured as well as its criticality to the overall risk profile of the bank. The precise timing will also depend on the bank-specific frequency requirements for risk management reporting, under both normal and stress/crisis situations, set based on the characteristics and overall risk profile of the bank.



	R45	R46	R47	P5
Fully compliant	3	2	2	2
Largely compliant	15	19	16	17
Materially non-compliant	12	9	12	11
Non-compliant	0	0	0	0
Average rating	2.7	2.8	2.7	2.7

As shown in the P5 bar, 7% of banks rated themselves as fully compliant, while 57% indicated that they were largely compliant, and 37% rated themselves as materially non-compliant. The average rating for this Principle was 2.7.

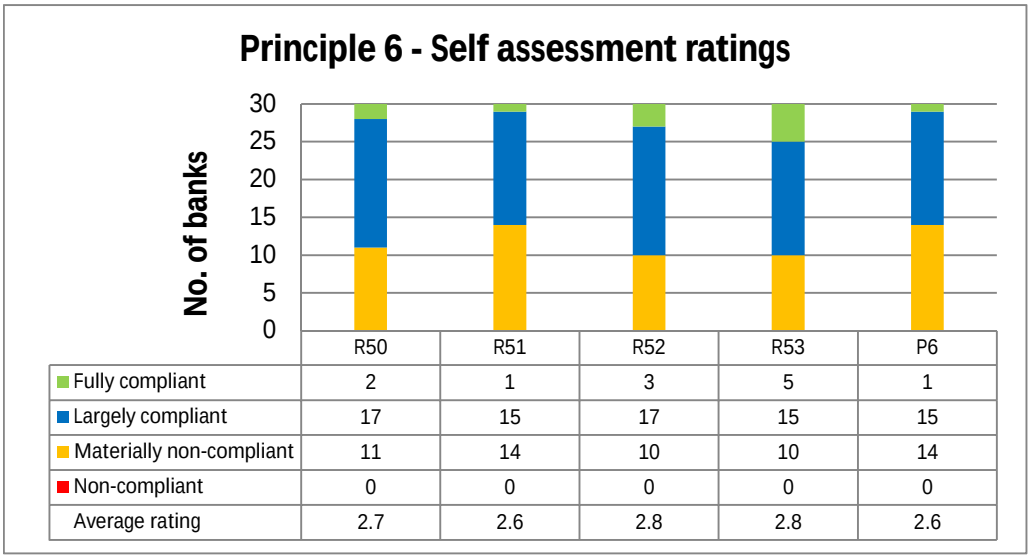
Of the 28 banks that did not rate themselves as fully compliant, 87% expected to comply by the January 2016 deadline, with expected compliance dates that ranged from September 2015 to January 2016. One of the remaining four banks (13%) had an estimated compliance date of December 2016. Banks indicated that they would not be able to fully comply by the deadline due to multi-year in-flight IT infrastructure initiatives.

Three requirements supported the assessment of this Principle. The average rating assigned to each requirement ranged from 2.7 to 2.8. As shown in the chart, both R47 (capabilities of rapidly producing risk data in stress situations) and R45 (documented timeliness requirements in normal and stress situations) received 12 materially non-compliant ratings, which represented the lowest-rated requirement under this Principle.

The main challenges and issues regarding timely data aggregation include:

- Need to enhance timeliness especially in stress/crisis situations, considering trade-offs between timeliness and other Principles (accuracy and integrity, completeness and adaptability), mainly due to heavy reliance on manual workarounds in data aggregation processes, including reconciliation (related to R47 and 46).
- Comprehensive identification and documentation of timeliness requirements under both normal and stress situations (related to R45).

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.



	R50	R51	R52	R53	P6
Fully compliant	2	1	3	5	1
Largely compliant	17	15	17	15	15
Materially non-compliant	11	14	10	10	14
Non-compliant	0	0	0	0	0
Average rating	2.7	2.6	2.8	2.8	2.6

As shown in the P6 bar, the population was nearly evenly split between largely compliant and materially non-compliant ratings, while 3% (one bank) rated itself as fully compliant. This bank also mentioned that its process allows for the incorporation of new developments. The average rating for this Principle was 2.6, which was the second lowest among the 11 Principles.

Of the 29 banks that did not rate themselves as fully compliant, 79% expected to comply by the January 2016 deadline, with expected compliance dates that ranged from June 2015 to January 2016. One of the remaining six banks (21%) had an estimated compliance date of 2017. Banks indicated that they would not be able to fully comply by the deadline due to ongoing multi-year IT infrastructure initiatives.

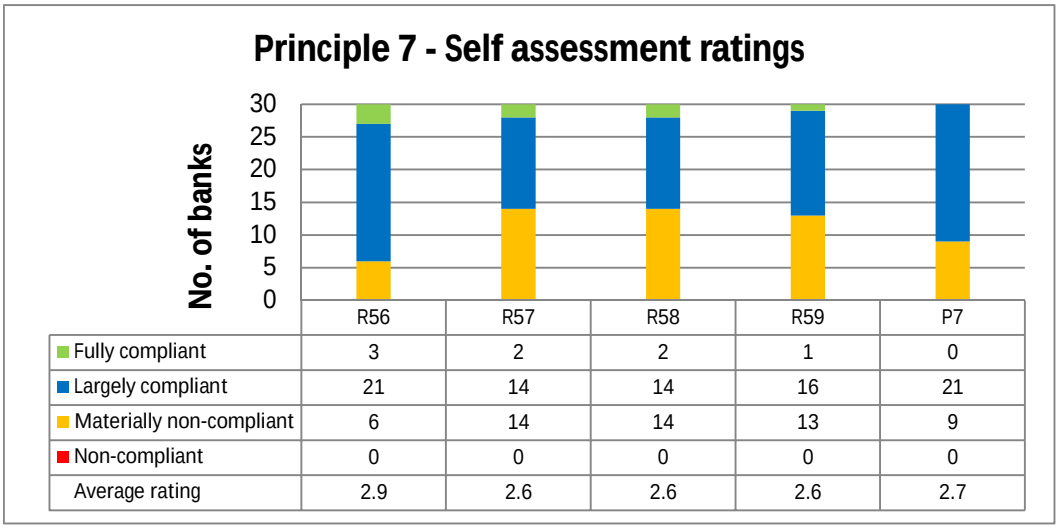
Four requirements supported the assessment of this Principle. The average rating assigned to each requirement ranged from 2.6 to 2.8. As shown in the chart, R51 (customisation of data) received 14 materially non-compliant ratings, which represented the lowest-rated requirement under this Principle.

The main challenges and issues regarding data adaptability include:

- Heavy reliance on manual workarounds, limited capabilities to meet ad hoc requests and adopt internal/external changes, and inflexible systems and processes (related to R50–53).

3.3 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.



	R56	R57	R58	R59	P7
Fully compliant	3	2	2	1	0
Largely compliant	21	14	14	16	21
Materially non-compliant	6	14	14	13	9
Non-compliant	0	0	0	0	0
Average rating	2.9	2.6	2.6	2.6	2.7

As shown in the P7 bar, 70% of banks rated themselves as largely compliant, while the remaining 30% rated themselves as materially non-compliant. The average rating for this Principle was 2.7.

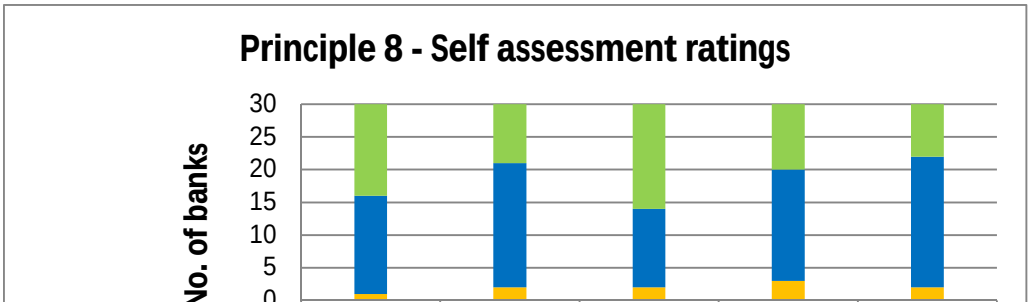
While no banks rated themselves as fully compliant, 83% expected to comply by the January 2016 deadline, with expected compliance dates that ranged from December 2014 to January 2016. Two of the remaining five banks (17%) had estimated compliance dates of December 2017, two years after the deadline.

Four requirements supported the assessment of this Principle. The average rating assigned to each requirement ranged from 2.6 to 2.9, with three of the requirements having the same lowest average rating under this Principle. As shown in the chart, those three requirements, R57 (automated and manual edit and reasonableness checks), R58 (integrated procedure for identifying and reporting data errors), and R59 (accuracy requirements for regular and stress cases), received 14, 14 and 13 materially non-compliant ratings, respectively.

The main challenges and issues regarding reporting accuracy include:

- An overreliance on manual processes to generate and reconcile risk reports (related to R57).
- Weaknesses or inconsistencies in the design and implementation of reconciliation processes and data quality exception reporting (related to R58 and R56).
- Lack of formal, documented accuracy requirements and/or reconciliation procedures (related to R59).

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.



	R62	R63	R64	R65	P8
Fully compliant	14	9	16	10	8
Largely compliant	15	19	12	17	20
Materially non-compliant	1	2	2	3	2
Non-compliant	0	0	0	0	0
Average rating	3.4	3.2	3.5	3.2	3.2

As shown in the P8 bar, 27% of banks rated themselves as fully compliant, 67% rated themselves as largely compliant and 7% rated themselves as materially non-compliant. The average rating for this Principle was 3.2, the second-highest rating among the 11 Principles.

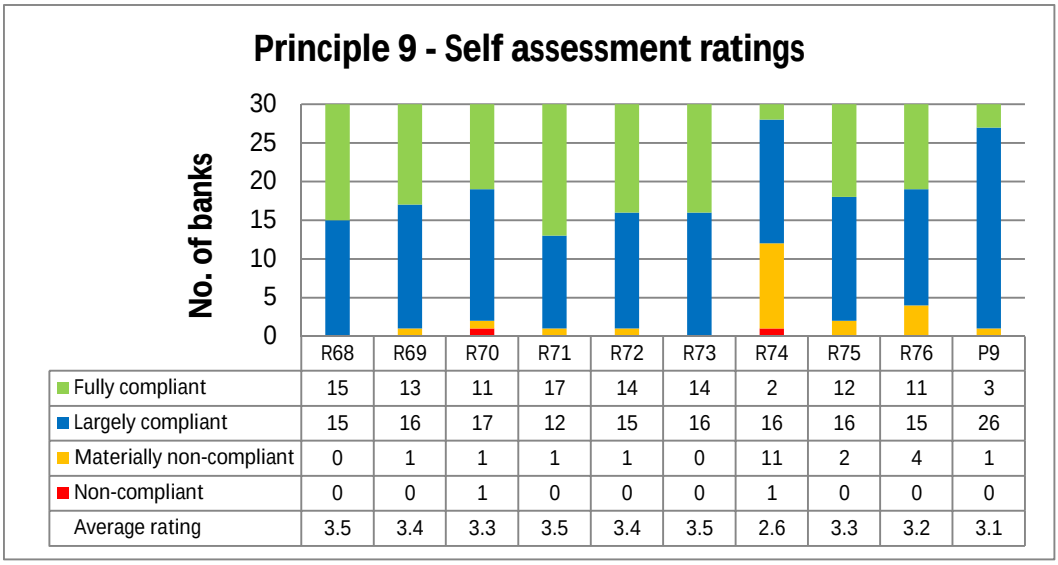
Of the 22 banks that did not rate themselves as fully compliant, 91% expected to comply by the January 2016 deadline, with expected compliance dates that ranged from December 2014 to January 2016. The two materially non-compliant banks (9%) had estimated compliance dates of December 2016 and January 2017, approximately one year after the deadline.

Four requirements supported the assessment of this Principle. The average rating assigned to each requirement ranged from 3.2 to 3.5. As shown in the chart, there were a few materially non-compliant ratings across all requirements under this Principle. However, as depicted in the chart on page 22, several banks rated themselves higher on this Principle than on Principle 4, and as such may have overstated their current level of compliance with Principle 8. Banks need to comply with Principle 4 before they consider themselves compliant with this Principle.

The main challenges and issues regarding reporting comprehensiveness include:

- Limitations in stress testing, scenario analysis and emerging risk identification and reporting capabilities (related to R65).
- The need to fully incorporate risk appetite into risk reporting (related to R63).

Principle 9 – Clarity and usefulness – Risk management reports should communicate information in a clear and concise manner. Reports should be easy to understand yet comprehensive enough to facilitate informed decision-making. Reports should include meaningful information tailored to the needs of the recipients.



	R68	R69	R70	R71	R72	R73	R74	R75	R76	P9
Fully compliant	15	13	11	17	14	14	2	12	11	3
Largely compliant	15	16	17	12	15	16	16	16	15	26
Materially non-compliant	0	1	1	1	1	0	11	2	4	1
Non-compliant	0	0	1	0	0	0	1	0	0	0
Average rating	3.5	3.4	3.3	3.5	3.4	3.5	2.6	3.3	3.2	3.1

As shown in the P9 bar, 10% of banks rated themselves as fully compliant, while 87% rated themselves as largely compliant, and one bank (3%) rated itself as materially non-compliant. The average rating for this Principle was 3.1, which was the third highest rating among the 11 Principles.

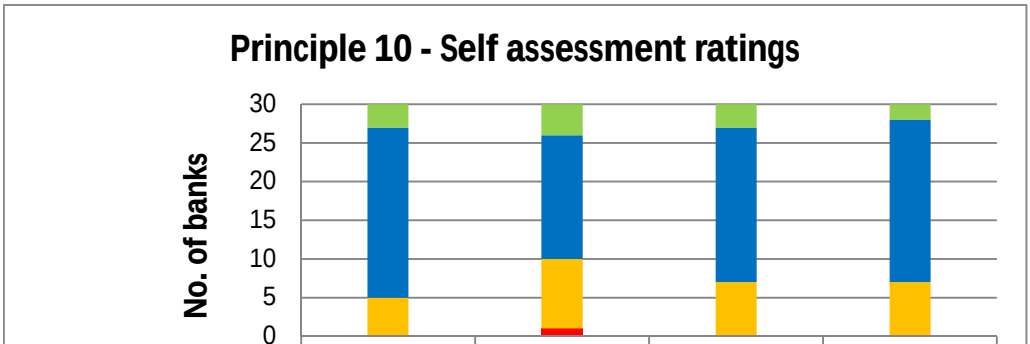
Of the 27 banks that did not rate themselves as fully compliant, 96% expected to comply by the January 2016 deadline, with expected compliance dates that ranged from December 2014 to January 2016. The remaining bank had an estimated compliance date of January 2017.

Nine requirements supported the assessment of this Principle. The average rating assigned to each requirement ranged from 2.6 to 3.5. As shown in the chart, R74 (inventory and classification of risk data items) had 11 materially non-compliant ratings and one non-compliant rating, which represented the lowest-rated requirement under this Principle. R70 (differentiated information needs of the board, senior management, etc) had one materially non-compliant rating and one non-compliant rating.

The main challenges and issues regarding reporting clarity and usefulness include:

- Lack of a documented and formalised single data inventory, dictionary and/or classification of reported risk data items at the group level (related to R74).
- Lack of formal processes and policies to recognise the differing information needs of the board, senior management and the other levels of the organisation (related to R70).
- Need to expand the feedback process to include all report recipients (related to R76).
- Risk reports lack supporting analytics and/or qualitative insights to explain trends and underlying data challenges (related to R69 and R75).

Principle 10 – Frequency – The board and senior management (or other recipient 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.



	R79	R80	R81	P10
Fully compliant	3	4	3	2
Largely compliant	22	16	20	21
Materially non-compliant	5	9	7	7
Non-compliant	0	1	0	0
Average rating	2.9	2.8	2.9	2.8

As shown in the P10 bar, 7% of banks rated themselves as fully compliant, 70% rated themselves as largely compliant and 23% rated themselves as materially non-compliant. The average rating for this Principle was 2.8.

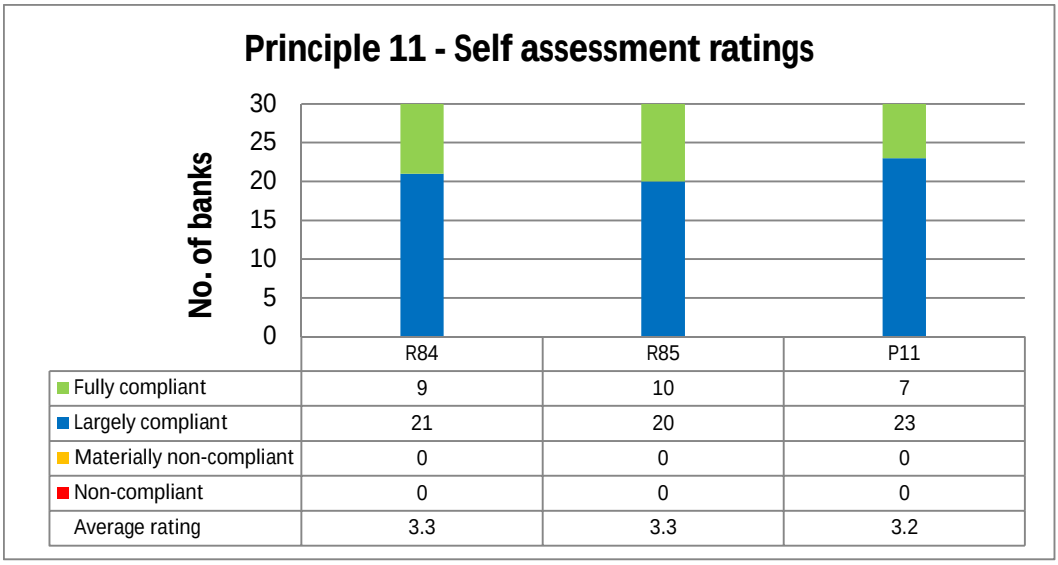
Of the 28 banks that did not rate themselves as fully compliant, 86% expected to comply by the January 2016 deadline, with expected compliance dates that ranged from December 2014 to January 2016. One of the remaining four banks (14%) had an estimated compliance date of December 2016.

Three requirements supported the assessment of this Principle. The average rating assigned to each requirement ranged from 2.8 to 2.9. As shown in the chart, R80 (routine test to produce accurate reports in stress conditions) had nine materially non-compliant ratings and one non-compliant rating, which represented the lowest-rated requirement under this Principle.

The main challenges and issues regarding reporting frequency include:

- Lack of formal processes, particularly in stress/crisis situations, for routinely testing the bank's capabilities to produce accurate reports within established time frames (related to R80).
- The frequency of ad hoc stress/scenario analysis and reporting is hampered by the lack of robust data aggregation capabilities, including an overreliance on manual processes that often prevents banks from generating reports in a very short period of time (related to R79 and R81).

Principle 11 – Distribution – Risk management reports should be distributed to relevant parties while ensuring confidentiality is maintained.



	R84	R85	P11
Fully compliant	9	10	7
Largely compliant	21	20	23
Materially non-compliant	0	0	0
Non-compliant	0	0	0
Average rating	3.3	3.3	3.2

As shown in the P11 bar, 23% of banks rated themselves as fully compliant with Principle 11, and 77% rated themselves as largely compliant. No banks reported material non-compliance. The average rating for this Principle was 3.2, the highest among the 11 Principles.

Of the 23 banks that did not rate themselves as fully compliant, 100% expected to comply by the January 2016 deadline, with expected compliance dates that ranged from December 2013 to January 2016.

Two requirements supported the assessment of this Principle. The average rating assigned to each requirement was 3.3. As shown in the chart, neither requirement had any materially non-compliant ratings. However, banks may have tended to overstate their ratings on this Principle (see next section).

Banks did not mention any significant challenges and issues regarding distribution requirements.

4. Supervisory assessments

This section presents key comments by national supervisors and the WGSS on the three broad areas covered by the Principles (governance and infrastructure, risk data aggregation and risk reporting).

Supervisors understand that many banks found it challenging to complete the questionnaire and made significant efforts in collecting inputs, in part because the questionnaire was circulated shortly after issuance of the Principles. Although the WGSS is confident that the questionnaire results broadly reflect the current state of implementation based on members' knowledge of participating banks, several caveats nevertheless apply to the results. For example, the outcomes in this paper are based on self-assessments by banks that were conducted on a best efforts basis. Moreover, the ratings assigned as part of the self-assessment process (ranging in compliance status from 4 (best) to 1 (worst)) were defined broadly and may therefore have been interpreted more or less conservatively across banks. In addition, although national supervisors reviewed responses and discussed them with banks in their jurisdictions, they were not asked to validate the accuracy of the banks' ratings or comments, nor did they assess the potential differences in the level of rigor applied by each bank or differences in

home/host supervisory approaches. The results may, therefore, be best understood as providing a snapshot of banks' overall preparedness to comply with the Principles, as well as the relative challenges faced.

Participating supervisors believe that banks made a good-faith effort to accurately assess their current state of implementation, including weaknesses. However, supervisors and the WGSS identified the following weaknesses in addition to those identified by participating banks.

First, in many cases banks' self-assessment scope was limited to the group level and did not take into account each material business unit or entity within the group. Supervisors agree that these Principles apply not only at the group level, but also to all material business units or entities within the group. Second, when rating themselves on risk reporting Principles, a number of banks only focused on the quality of risk reports to senior management and the board (not including middle management). Third, there is evidence that many banks assessed only a few types of risk, such as credit risk and market risk, while not comprehensively covering other types of risk, such as liquidity risk, operational risk and other risks. Fourth, very few banks offered insights into their definitions of materiality or tolerance level for manual versus automated processes for risk data aggregation and reporting. Some banks may have used those definitions to justify higher compliance ratings than may be warranted.

These self-assessment scope limitations raise concerns that the ratings chosen by banks may not accurately reflect their compliance status, covering all material group entities, all levels of management and all types of material risk. In this regard, banks may have in some instances overstated their ratings. At the core of the rating distributions (2–3), as would be expected if banks' assessments are correct, banks that rated themselves as materially non-compliant described critical issues and remediation plans more thoroughly than those that rated themselves as largely compliant. Furthermore, some of the banks that rated themselves as largely compliant might be implicitly taking advance credit for projects to upgrade their risk data frameworks which are far from complete. It is also noteworthy that 10 banks were not committed to full compliance with at least one Principle by the January 2016 deadline. In addition, in other cases the expected compliance dates set by some banks seemed to be overly optimistic, notably for banks rating themselves 2 on a given principle and yet stating that they will be fully compliant before the deadline. Supervisors and the WGSS should closely analyse and follow up on these points during 2014.

Governance and infrastructure

G-SIBs appear to have escalated risk data issues to a priority level for corporate leadership. In terms of current compliance status, however, they still have to unify the governance and align the architecture of multiple risk MIS modules, which may cover different subsets of risk types or entities and have uneven data capabilities and output/report quality. Thus, data aggregation and reporting frameworks at most G-SIBs remain inadequately documented and somewhat fragmented. Indeed, all five banks that rated themselves as materially non-compliant with Principle 1 (governance) reported such shortcomings. A few of these institutions are also still transitioning from major mergers and acquisitions undertaken over the past five to six years.

Principle 2 (data architecture and infrastructure) had the lowest average rating, which signals that this is a critical area in need of improvement, notably in terms of unifying and rationalising the dictionaries and taxonomies of risk data repositories, as well as establishing clear risk data ownership and responsibility over the attendant quality controls. At the majority of G-SIBs, the scope of these controls and the enforcement of group data quality policies by central functions are incomplete, and the mandates of central functions vis-à-vis business lines and local units are unclear. Caution is warranted even for institutions that rated themselves 3 or 4 on some of the underlying requirements, as their stated action plans may still be in the design/pilot phase and not yet tested in real time.

Risk data aggregation capabilities

A number of supervisors agree with their banks' self-assessments for risk data aggregation Principles and are aware of the challenges faced by their banks. The low average ratings (2.6–2.7) for Principles 3–6 show that banks have significant gaps in terms of data accuracy, completeness, timeliness and adaptability. Banks will have to make significant efforts to address these gaps, which are also likely to affect risk reporting capabilities. Supervisors believe that banks are generally more able to ensure completeness of risk data than accuracy of risk data. A number of banks are dependent on manual processes to support their risk data aggregation, and supervisors' view is that these banks may struggle to aggregate risk data in a timely and accurate manner during stress/crisis situations.

A number of supervisors also feel that their banks have not taken into account the impact of challenges related to governance arrangements and IT systems when rating themselves on Principles 3–6. For example, some banks indicated that they do not materially comply with Principles 1 (governance) and 2 (data architecture and IT infrastructure), but then rated themselves largely compliant with Principle 3 (accuracy and integrity). Supervisors believe that risk data generally are less accurate than accounting data in many banks, and data inspection processes such as reconciliations can be lengthy and complex to carry out. Supervisors also note that the majority of banks identified and documented timeliness requirements based on the nature and potential volatilities of risk types and metrics, but further enhancement of timeliness is necessary for some banks, especially in stress situations.

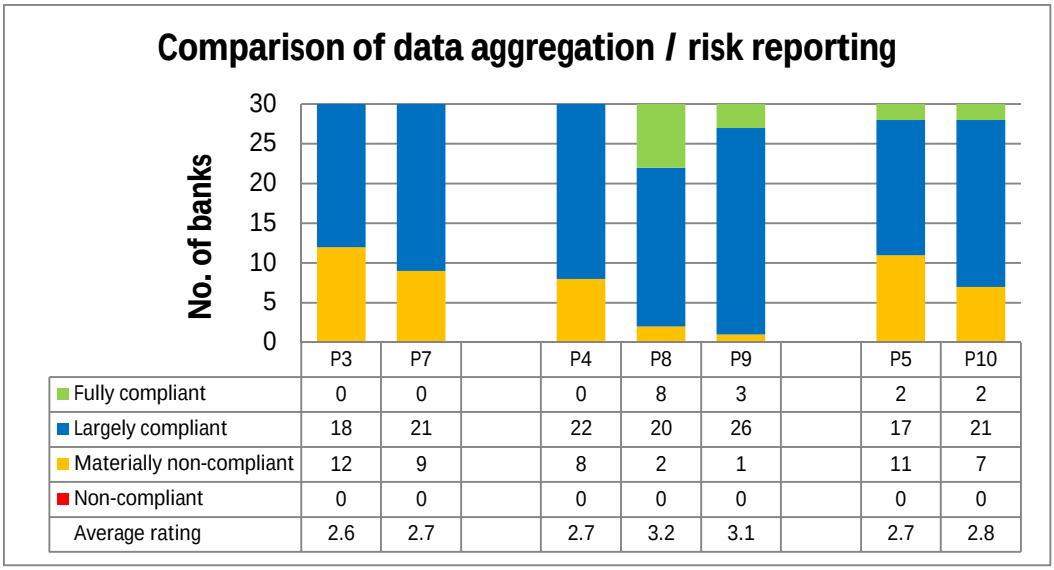
Adaptability had the second lowest average rating among all Principles, and only one bank reported full compliance with this Principle at this stage. Key common gaps for banks that are currently materially non-compliant or largely compliant were: (i) limitations in coverage and timeliness, especially in stress/crisis situations; and (ii) manual workarounds necessary for meeting ad hoc requests and/or adapting to internal and external changes.

Risk reporting practices

Although most supervisors concluded that their banks' responses were broadly credible in the area of governance and infrastructure and risk data aggregation capabilities, supervisors noted that most banks failed to take into account the interdependencies among the three areas of the Principles. Many banks focused primarily on quality of risk reports for senior management and the board when rating themselves on risk reporting principles. In these cases, the banks rated themselves higher on the risk reporting Principles than they did on the other Principles.[3] These inconsistencies, examples of which are provided below, suggest that some of the fully compliant and largely compliant ratings assigned to risk reporting Principles may have overstated banks' actual level of compliance.

More than 50% of the banks rated themselves higher on one or more risk reporting Principles (Principles 7–11) than they did on Principle 2 (data architecture and IT infrastructure). In addition, one third of the banks rated themselves higher on one or more risk reporting Principles than they did on Principle 1 (governance). These banks included the seven that rated themselves as fully compliant with Principle 8 (comprehensiveness). In most cases, the ratings differed by one level. However, three of the banks that rated themselves as fully compliant with Principle 8 rated themselves as materially non-compliant with Principle 2.

[3] Section 26 of the Principles states that a strong governance framework, risk data architecture and IT infrastructure are "preconditions to ensure compliance with the other principles". Section 35 of the Principles states that "meeting data aggregation principles is necessary to meet reporting expectations".



	P3	P7		P4	P8	P9		P5	P10
Fully compliant	0	0		0	8	3		2	2
Largely compliant	18	21		22	20	26		17	21
Materially non-compliant	12	9		8	2	1		11	7
Non-compliant	0	0		0	0	0		0	0
Average rating	2.6	2.7		2.7	3.2	3.1		2.7	2.8

Definition of Principles: P3 = accuracy and integrity; P7 = accuracy; P4 = completeness; P8 = comprehensiveness; P9 = clarity and usefulness; P5 = timeliness; P10 = frequency.

As illustrated in the chart above, some data aggregation and risk reporting Principles closely align with each other because complying with the former is a pre-requisite to complying with the latter. Principles 3 and 7 both address accuracy and integrity. Principles 4, 8 and 9 address completeness, comprehensiveness and clarity/usefulness. Principles 5 and 10 address the ability to produce reports in a timely manner at an appropriate frequency. However, the chart shows that banks generally assigned themselves higher ratings on the risk reporting Principles than they did on the corresponding data aggregation Principles. This includes a few banks that rated themselves as fully compliant on Principle 8 and materially non-compliant on one or more data aggregation Principles.

Finally, although banks did not mention any significant challenges and issues regarding Principle 11 (distribution), the WGSS identified the following technical issues:

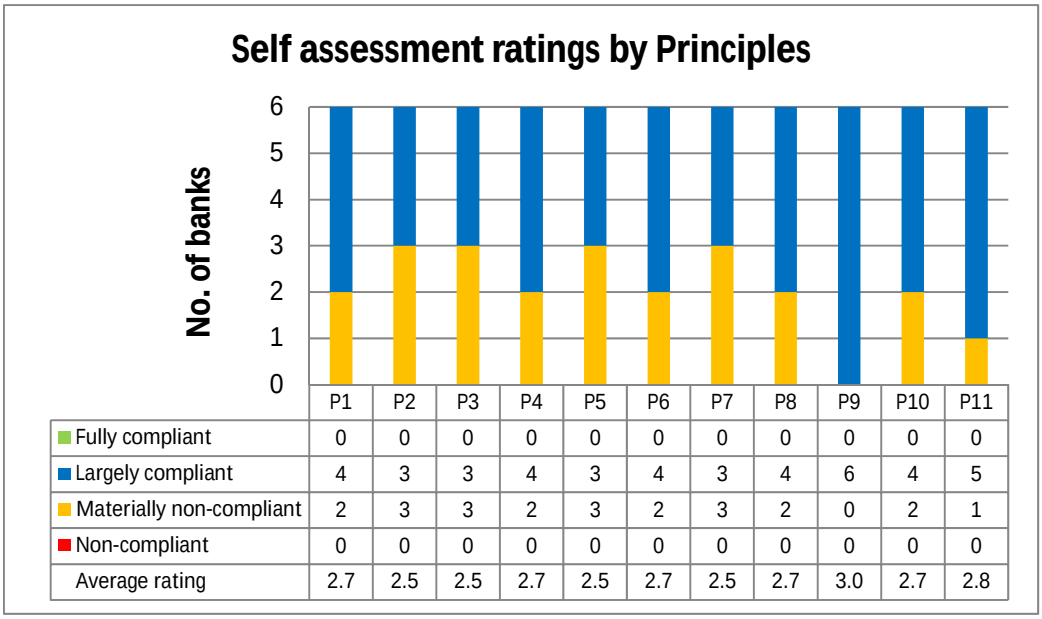
- Integrating the distribution processes of all relevant units, ie enhancing automation to support rapid data collection and analysis (related to R84).
- Lack of formal procedures to confirm that the relevant recipients receive timely reports (related to R85).

5. Other large banks' self-assessments

The Basel Committee invited national supervisors to decide on a voluntary basis to include other large banks in the exercise. Four national supervisors asked other large banks that were not G-SIBs to join the exercise. Consequently, six other large banks participated in this exercise. The WGSS wanted to assess whether a compliance gap existed between G-SIBs and other large banks to help national supervisors apply the Principles to these banks in coming years. There is a possibility that these six banks are not necessarily a representative sample of all other large banks, considering the limited number of jurisdictions and banks participating in the exercise.

5.1 Overview of compliance reported by other large banks

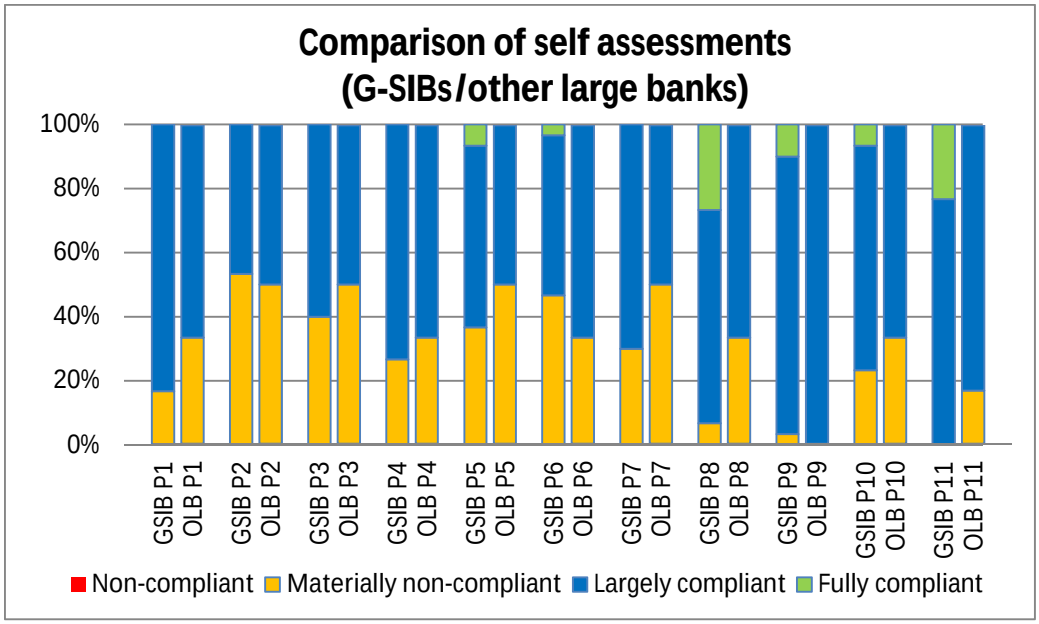
As shown in the chart below, more than half of the other large banks reported that they were largely compliant with each Principle. No banks rated themselves as fully compliant or non-compliant with any of the Principles. All but one of the banks expected to comply with the Principles by January 2016, with time frames ranging from June 2014 to January 2016.



	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11
Fully compliant	0	0	0	0	0	0	0	0	0	0	0
Largely compliant	4	3	3	4	3	4	3	4	6	4	5
Materially non-compliant	2	3	3	2	3	2	3	2	0	2	1
Non-compliant	0	0	0	0	0	0	0	0	0	0	0
Average rating	2.7	2.5	2.5	2.7	2.5	2.7	2.5	2.7	3.0	2.7	2.8

5.2 Comparison of other large banks with G-SIBs

The chart below shows a comparison between the outcomes of the self-assessment of other large banks with the self-assessments of G-SIBs. In general, the Principles and requirements related to risk reporting had higher scores for both G-SIBs and other large banks than the other Principles. Broadly speaking, other large banks had slightly wider compliance gaps than G-SIBs across all Principles.



6. Conclusions: supervisory plans and next steps

By completing the bank stocktaking self-assessment questionnaire, national supervisors and the WGSS have finished the first step of the preparation period. Banks demonstrated that they understand the importance of the Principles and are committed to enhancing their data aggregation and reporting capabilities. However, each G-SIB's reported compliance status with each Principle still varies. Indeed, many banks are facing difficulties in establishing strong data aggregation governance, architecture and processes, which are the initial stage of implementation. Instead they resort to extensive manual workarounds. The key takeaway is that manual aggregation/reconciliation, even if it somehow results in acceptable risk reports, cannot substitute for strong aggregation capabilities, and over-reliance on such manual workarounds impairs banks' risk data aggregation and reporting. In terms of the deadline, 10 G-SIBs mentioned that they currently expect to not fully comply with at least one Principle by 1 January 2016. Some of these banks noted that this is due to large, ongoing, multi-year, in-flight IT and data-related projects. Thus, many banks need to make significant progress in order to meet the requirements.

According to the stocktaking questionnaire for national supervisors, all participating supervisory authorities are committed to achieving full compliance by G-SIBs with the Principles by 1 January 2016. The stocktaking exercise shows that supervisory authorities are already doing meaningful work in overseeing the Principles. Supervisors review relevant aspects of banks' risk data aggregation and reporting frameworks in their existing supervisory programmes and through their assessment of related banking areas. In addition, supervisory authorities have a broad range of tools and remedial actions to enforce the Principles and have the expertise/resources to monitor banks' progress towards implementation. Based on this exercise, it is recommended that supervisory authorities consider enhancing their efforts to: (i) fully integrate the Principles in a comprehensive way within their supervisory programmes; (ii) test banks' capabilities to aggregate and produce reports in stress/crisis situations, including resolution; (iii) conduct thematic reviews; and (iv) develop concrete supervisory plans or other supervisory tools for 2014 and 2015.

With regard to next steps, in order to ensure that G-SIBs will fully comply with the Principles by the deadline, national supervisors will investigate the root causes of non-compliance, and use supervisory tools or appropriate discretionary measures depending on banks' situations. National supervisors and the WGSS should ensure that banks move further towards implementation in 2014, bearing in mind that if banks are to produce high-quality risk data and risk reports, they need to build up strong risk data governance and architecture and robust aggregation capabilities. As relevant, that work will be coordinated by the WGSS with the implementation of other G-SIB/D-SIB standards under the Regulatory Consistency Assessment Programme (RCAP). In the two remaining years before entry into force, the WGSS is contemplating the following steps:

(a) Conduct a self-assessment survey of banks in a reduced form and a thematic review of the requirements with lowest scores

(b) National supervisors' review of banks' self-assessments

(c) Stress tests to require banks to complete a risk data aggregation template within a limited time

Annex 1: 30 G-SIBs identified in 2011 and 2012[4]

Jurisdiction	G-SIBs
Belgium	Dexia*
China	Bank of China
France	BNP Paribas Group BPCE Group Crédit Agricole Société Générale
Germany	Commerzbank Deutsche Bank
Italy	Unicredit Group
Japan	Mitsubishi UFJ FG Mizuho FG Sumitomo Mitsui FG
Netherlands	ING Bank
Spain	BBVA Santander
Sweden	Nordea
Switzerland	Credit Suisse UBS
UK	Barclays HSBC Lloyds Banking Group Royal Bank of Scotland Standard Chartered
US	Bank of America Bank of New York Mellon Citigroup Goldman Sachs JPMorgan Chase Morgan Stanley State Street Wells Fargo

* Dexia is undergoing an orderly resolution process and didn't participate in this survey.

[4] Banks identified as G-SIBs in November 2011 or November 2012 must comply with the Principles by January 2016. See the BCBS Principles at www.bis.org/publ/bcbs239.pdf.

Annex 2: List of 11 Principles and 87 requirements[5]

Principles		Requirements	
Governance/infrastructure	1. Governance	1	Framework established
		2	Approval of the framework and resources deployed
		3	Data quality risks as part of risk framework
		4	Policies on data and risk management
		5	Full documentation and validation
		6	Independent validation by qualified staff
		7	Consideration as part of any new initiatives
		8	Assessment of the data aggregation process in case of acquisitions
		9	Unaffected by bank's group structure
		10	Aware of technical limitations
		11	IT strategy addresses improvements
		12	Sufficient financial and human resources
		13	Board sets reporting requirements
		14	Board's awareness of limitations
		15	Board's awareness of implementation and ongoing compliance
		16	Overall assessment
		17	Expected date of full compliance
	2. Data architecture and IT infrastructure	18	Business' continuity planning and impact analysis
		19	Data taxonomies
		20	Responsibilities on ownership, quality of data and information
		21	Role of the business owner
		22	Adequate controls through the life cycle of data
		23	Overall assessment
		24	Expected date of full compliance
Risk data aggregation capabilities	3. Accuracy and integrity	25	Controls as to accounting data
		26	Mitigants and controls for manual processes
		27	Reconciliation with different sources
		28	Access to risk data of the bank's risk personnel
		29	Dictionary
		30	Balance between automated and manual systems
		31	Documentation of risk data aggregation processes
		32	Measurement and monitoring processes
		33	For all material risks
		34	Process to rectify poor data quality
		35	Overall assessment
		36	Expected date of full compliance
	4. Completeness	37	Process to identify groups to report risks
		38	All material risk data included
		39	Documentation of approaches to aggregate exposures

[5] Including "Overall assessment" and "Expected date of full compliance" of each principle

		40	Measurement and monitoring of all material risk data
		41	Exceptions properly identified and explained
		42	Process to rectify completeness issues
		43	Overall assessment
		44	Expected date of full compliance
	5. Timeliness	45	Documented timeliness requirements in normal and stress situations
		46	Capabilities to produce timely information to meet reporting requirements
		47	Capabilities of rapidly producing risk data in stress situations
		48	Overall assessment
		49	Expected date of full compliance
	6. Adaptability	50	Ad hoc data requests
		51	Customisation of data
		52	Incorporate new internal or external developments
		53	Incorporate regulatory changes
		54	Overall assessment
		55	Expected date of full compliance
Risk reporting practices	7. Accuracy	56	Requirements and processes to reconcile reports to risk data
		57	Automated and manual edit and reasonableness checks
		58	Integrated procedure for identifying and reporting data errors
		59	Accuracy requirements for regular and stress cases
		60	Overall assessment
		61	Expected date of full compliance
	8. Comprehensiveness	62	Reporting in line with business model and risk profile
		63	Emerging risks included, in the context of the risk appetite
		64	Status of measures agreed to deal with specific risks
		65	Forecasts and stress tests
		66	Overall assessment
		67	Expected date of full compliance
	9. Clarity and usefulness	68	Reports tailored to recipients' needs
		69	Balance between data analysis and qualitative explanations
		70	Differentiated information needs of the board, senior management, etc
		71	Board determines its own reporting requirements
		72	Feedback by the board to senior management
		73	Senior management determines its own reporting requirements
		74	Inventory and classification of risk data items
		75	Balance between data and recommendations, conclusions, interpretations
		76	Periodic confirmation of relevance and completeness
		77	Overall assessment
		78	Expected date of full compliance
	10. Frequency	79	Requirements for how quickly reports are produced in normal/stress times
		80	Routine test to produce accurate reports in stress conditions
		81	Availability of all critical exposure reports shortly in stress situations
		82	Overall assessment
		83	Expected date of full compliance
	11. Distribution	84	Timely dissemination of reports balanced with appropriate confidentiality
		85	Periodic confirmation of the timeliness of reports
		86	Overall assessment
		87	Expected date of full compliance

Annex 3: Average ratings sorted P1–P11

Principle	Question	Number of banks for each rating				Total	Average	Brief explanation of each requirement
		1 NC	2 MNC	3 LC	4 FC			
P1	R1	0	8	19	3	30	2.83	Framework established
P1	R2	0	16	12	2	30	2.53	Approval of the framework and resources deployed
P1	R3	0	7	21	2	30	2.83	Data quality risks as part of risk framework
P1	R4	0	6	23	1	30	2.83	Policies on data and risk management
P1	R5	0	13	16	1	30	2.60	Full documentation and validation
P1	R6	1	5	16	8	30	3.03	Independent validation by qualified staff
P1	R7	1	3	21	5	30	3.00	Consideration as part of any new initiatives
P1	R8	1	7	13	9	30	3.00	Assessment of the data aggregation process in case of acquisitions
P1	R9	0	8	17	5	30	2.90	Unaffected by bank's group structure
P1	R10	0	7	19	4	30	2.90	Aware of technical limitations
P1	R11	0	8	15	7	30	2.97	IT strategy addresses improvements
P1	R12	0	4	15	11	30	3.23	Sufficient financial and human resources
P1	R13	0	1	10	19	30	3.60	Board sets reporting requirements
P1	R14	0	5	19	6	30	3.03	Board's awareness of limitations
P1	R15	2	6	11	11	30	3.03	Board's awareness of implementation and ongoing compliance
P1	**P1**	**0**	**5**	**25**	**0**	**30**	**2.83**	**GOVERNANCE**
P2	R18	0	2	18	10	30	3.27	Business' continuity planning and impact analysis
P2	R19	0	20	9	1	30	2.37	Data taxonomies
P2	R20	0	10	17	3	30	2.77	Responsibilities on ownership, quality of data and information
P2	R21	0	18	11	1	30	2.43	Role of the business owner
P2	R22	0	14	14	2	30	2.60	Adequate controls through the life cycle of data
P2	**P2**	**0**	**16**	**14**	**0**	**30**	**2.47**	**DATA ARCHITECTURE AND IT INFRASTRUCTURE**
P3	R25	0	7	20	3	30	2.87	Controls as to accounting data
P3	R26	0	11	14	5	30	2.80	Mitigants and controls for manual processes
P3	R27	0	7	20	3	30	2.87	Reconciliation with different sources
P3	R28	0	7	21	2	30	2.83	Access to risk data of the bank's risk personnel
P3	R29	0	13	15	2	30	2.63	Dictionary
P3	R30	0	18	10	2	30	2.47	Balance between automated and manual systems
P3	R31	0	17	13	0	30	2.43	Documentation of risk data aggregation process
P3	R32	0	11	16	3	30	2.73	Measurement and monitoring processes
P3	R33	0	10	19	1	30	2.70	For all material risks
P3	R34	0	11	16	3	30	2.73	Process to rectify poor data quality
P3	**P3**	**0**	**12**	**18**	**0**	**30**	**2.60**	**ACCURACY AND INTEGRITY**
P4	R37	0	4	22	4	30	3.00	Process to identify groups to report risks
P4	R38	0	4	19	7	30	3.10	All material risk data included
P4	R39	0	10	14	6	30	2.87	Documentation of approaches to aggregate exposures
P4	R40	0	10	16	4	30	2.80	Measurement and Monitoring of all material risk data
P4	R41	0	11	16	3	30	2.73	Exceptions properly identified and explained
P4	R42	0	4	20	6	30	3.07	Process to rectify completeness issues
P4	**P4**	**0**	**8**	**22**	**0**	**30**	**2.73**	**COMPLETENESS**
P5	R45	0	12	15	3	30	2.70	Documented timeliness requirements in normal and stress situations
P5	R46	0	9	19	2	30	2.77	Capabilities to produce timely information to meet reporting requirements
P5	R47	0	12	16	2	30	2.67	Capabilities of rapidly producing risk data in stress situations
P5	**P5**	**0**	**11**	**17**	**2**	**30**	**2.70**	**TIMELINESS**
P6	R50	0	11	17	2	30	2.70	Ad hoc data requests
P6	R51	0	14	15	1	30	2.57	Customization of data
P6	R52	0	10	17	3	30	2.77	Incorporate new internal or external developments
P6	R53	0	10	15	5	30	2.83	Incorporate regulatory changes
P6	**P6**	**0**	**14**	**15**	**1**	**30**	**2.57**	**ADAPTABILITY**
P7	R56	0	6	21	3	30	2.90	Requirements and processes to reconcile reports to risk data
P7	R57	0	14	14	2	30	2.60	Automated and manual edit and reasonableness checks
P7	R58	0	14	14	2	30	2.60	Integrated procedure for identifying and reporting data errors
P7	R59	0	13	16	1	30	2.60	Accuracy requirements for regular and stress cases
P7	**P7**	**0**	**9**	**21**	**0**	**30**	**2.70**	**ACCURACY**
P8	R62	0	1	15	14	30	3.43	Reporting in line with business model and risk profile
P8	R63	0	2	19	9	30	3.23	Emerging risks included, in the context of the risk appetite.
P8	R64	0	2	12	16	30	3.47	Status of measures agreed to deal with specific risks
P8	R65	0	3	17	10	30	3.23	Forecasts and stress tests
P8	**P8**	**0**	**2**	**20**	**8**	**30**	**3.20**	**COMPREHENSIVENESS**
P9	R68	0	0	15	15	30	3.50	Reports tailored to recipients' needs
P9	R69	0	1	16	13	30	3.40	Balance between data analysis and qualitative explanations
P9	R70	1	1	17	11	30	3.27	Differentiated information needs of the board , senior management, etc
P9	R71	0	1	12	17	30	3.53	Board determines its own reporting requirements
P9	R72	0	1	15	14	30	3.43	Feedback by the board to senior management
P9	R73	0	0	16	14	30	3.47	Senior management determines its own reporting requirements
P9	R74	1	11	16	2	30	2.63	Inventory and classification of risk data items
P9	R75	0	2	16	12	30	3.33	Balance between data and recommendations, conclusions, interpretations
P9	R76	0	4	15	11	30	3.23	Periodic confirmation of relevance and completeness
P9	**P9**	**0**	**1**	**26**	**3**	**30**	**3.07**	**CLARITY AND USEFULNESS**
P10	R79	0	5	22	3	30	2.93	Requirements for how quickly reports are produced in normal/ stress times
P10	R80	1	9	16	4	30	2.77	Routine test to produce accurate reports in stress conditions
P10	R81	0	7	20	3	30	2.87	Availability of all critical exposure reports shortly in stress situations
P10	**P10**	**0**	**7**	**21**	**2**	**30**	**2.83**	**FREQUENCY**
P11	R84	0	0	21	9	30	3.30	Timely dissemination of reports balanced with appropriate confidentiality
P11	R85	0	0	20	10	30	3.33	Periodic confirmation of the timeliness of reports
P11	**P11**	**0**	**0**	**23**	**7**	**30**	**3.23**	**DISTRIBUTION**

Annex 4: Average ratings sorted worst to best

Principle	Question	Number of banks for each rating				Total	Average	Brief explanation of each requirement
		1 NC	2 MNC	3 LC	4 FC			
P2	R19	0	20	9	1	30	2.37	Data taxonomies
P2	R21	0	18	11	1	30	2.43	Role of the business owner
P3	R31	0	17	13	0	30	2.43	Documentation of risk data aggregation process
P2	**P2**	**0**	**16**	**14**	**0**	**30**	**2.47**	**DATA ARCHITECTURE AND IT INFRASTRUCTURE**
P3	R30	0	18	10	2	30	2.47	Balance between automated and manual systems
P1	R2	0	16	12	2	30	2.53	Approval of the framework and resources deployed
P6	R51	0	14	15	1	30	2.57	Customization of data
P6	**P6**	**0**	**14**	**15**	**1**	**30**	**2.57**	**ADAPTABILITY**
P1	R5	0	13	16	1	30	2.60	Full documentation and validation
P2	R22	0	14	14	2	30	2.60	Adequate controls through the life cycle of data
P3	**P3**	**0**	**12**	**18**	**0**	**30**	**2.60**	**ACCURACY AND INTEGRITY**
P7	R57	0	14	14	2	30	2.60	Automated manual edit and reasonableness checks
P7	R58	0	14	14	2	30	2.60	Integrated procedure for identifying and reporting data errors
P7	R59	0	13	16	1	30	2.60	Accuracy requirements for regular and stress cases
P3	R29	0	13	15	2	30	2.63	Dictionary
P9	R74	1	11	16	2	30	2.63	Inventory and classification of risk data items
P5	R47	0	12	16	2	30	2.67	Capabilities of rapidly producing risk data in stress situations
P3	R33	0	10	19	1	30	2.70	For all material risks
P5	R45	0	12	15	3	30	2.70	Documented timeliness requirements in normal and stress situations
P5	**P5**	**0**	**11**	**17**	**2**	**30**	**2.70**	**TIMELINESS**
P6	R50	0	11	17	2	30	2.70	Ad hoc data requests
P7	**P7**	**0**	**9**	**21**	**0**	**30**	**2.70**	**ACCURACY**
P3	R32	0	11	16	3	30	2.73	Measurement and monitoring processes
P3	R34	0	11	16	3	30	2.73	Process to rectify poor data quality
P4	R41	0	11	16	3	30	2.73	Exceptions properly identified and explained
P4	**P4**	**0**	**8**	**22**	**0**	**30**	**2.73**	**COMPLETENESS**
P2	R20	0	10	17	3	30	2.77	Responsibilities on ownership, quality of data and information
P5	R46	0	9	19	2	30	2.77	Capabilities to produce timely information to meet reporting requirements
P6	R52	0	10	17	3	30	2.77	Incorporate new internal or external developments
P10	R80	1	9	16	4	30	2.77	Routine test to produce accurate reports in stress conditions
P3	R26	0	11	14	5	30	2.80	Mitigants and controls for manual processes
P4	R40	0	10	16	4	30	2.80	Measurement and Monitoring of all material risk data
P1	R1	0	8	19	3	30	2.83	Framework established
P1	R3	0	7	21	2	30	2.83	Data quality risks as part of risk framework
P1	R4	0	6	23	1	30	2.83	Policies on data and risk management
P1	**P1**	**0**	**5**	**25**	**0**	**30**	**2.83**	**GOVERNANCE**
P3	R28	0	7	21	2	30	2.83	Access to risk data of the bank's risk personnel
P6	R53	0	10	15	5	30	2.83	Incorporate regulatory changes
P10	**P10**	**0**	**7**	**21**	**2**	**30**	**2.83**	**FREQUENCY**
P3	R25	0	7	20	3	30	2.87	Controls as to accounting data
P3	R27	0	7	20	3	30	2.87	Reconciliation with different sources
P4	R39	0	10	14	6	30	2.87	Documentation of approaches to aggregate exposures
P10	R81	0	7	20	3	30	2.87	Availability of all critical exposure reports shortly in stress situations
P1	R9	0	8	17	5	30	2.90	Unaffected by bank's group structure
P1	R10	0	7	19	4	30	2.90	Aware of technical limitations
P7	R56	0	6	21	3	30	2.90	Requirements and processes to reconcile reports to risk data
P10	R79	0	5	22	3	30	2.93	Requirements for how quickly reports are produced in normal/stress times
P1	R11	0	8	15	7	30	2.97	IT strategy addresses improvements
P1	R7	1	3	21	5	30	3.00	Consideration as part of any new initiatives
P1	R8	1	7	13	9	30	3.00	Assessment of the data aggregation process in case of acquisitions
P4	R37	0	4	22	4	30	3.00	Process to identify groups to report risks
P1	R6	1	5	16	8	30	3.03	Independent validation by qualified staff
P1	R14	0	5	19	6	30	3.03	Board's awareness of limitations
P1	R15	2	6	11	11	30	3.03	Board's awareness of implementation and ongoing compliance
P4	R42	0	4	20	6	30	3.07	Process to rectify completeness issues
P9	**P9**	**0**	**1**	**26**	**3**	**30**	**3.07**	**CLARITY AND USEFULNESS**
P4	R38	0	4	19	7	30	3.10	All material risk data included
P8	**P8**	**0**	**2**	**20**	**8**	**30**	**3.20**	**COMPREHENSIVENESS**
P1	R12	0	4	15	11	30	3.23	Sufficient financial and human resources
P8	R63	0	2	19	9	30	3.23	Emerging risks included, in the context of the risk appetite.
P8	R65	0	3	17	10	30	3.23	Forecasts and stress tests
P9	R76	0	4	15	11	30	3.23	Periodic confirmation of relevance and completeness
P11	**P11**	**0**	**0**	**23**	**7**	**30**	**3.23**	**DISTRIBUTION**
P2	R18	0	2	18	10	30	3.27	Business' continuity planning and impact analysis
P9	R70	1	1	17	11	30	3.27	Differentiated information needs of the board , senior management, etc.
P11	R84	0	0	21	9	30	3.30	Timely dissemination of reports balanced with appropriate confidentiality
P9	R75	0	2	16	12	30	3.33	Balance between data and recommendations, conclusions, interpretations
P11	R85	0	0	20	10	30	3.33	Periodic confirmation of the timeliness of reports
P9	R69	0	1	16	13	30	3.40	Balance between data analysis and qualitative explanations
P8	R62	0	1	15	14	30	3.43	Reporting in line with business model and risk profile
P9	R72	0	1	15	14	30	3.43	Feedback by the board to senior management
P8	R64	0	2	12	16	30	3.47	Status of measures agreed to deal with specific risks
P9	R73	0	0	16	14	30	3.47	Senior management determines its own reporting requirements
P9	R68	0	0	15	15	30	3.50	Reports tailored to recipients' needs
P9	R71	0	1	12	17	30	3.53	Board determines its own reporting requirements
P1	R13	0	1	10	19	30	3.60	Board sets reporting requirements

Members of the Working Group on SIB Supervision (WGSS)

Chair: Fernando Vargas (Bank of Spain)

Canada	James Dennison	Office of the Superintendent of Financial Institutions
China	Zhangjun Wu	China Banking Regulatory Commission
France	Olya Ranguelova	French Prudential Supervision and Resolution Authority
Germany	Stefan Iwankowski	Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
	Tobias Volk	Deutsche Bundesbank
Hong Kong SAR	Sunny Yung	Hong Kong Monetary Authority
Italy	Angelo Carriero	Bank of Italy
Japan	Mitsutoshi Adachi	Bank of Japan
	Toru Sanada	Financial Services Agency
Mexico	Efrain Solorio	National Banking and Securities Commission
Netherlands	Truus Stadt	Netherlands Bank
Russia	Marina Eminova	Central Bank of the Russian Federation
Saudi Arabia	Syed Hassan Mehdi	Saudi Arabian Monetary Agency
Spain	Cristina Iglesias-Sarria	Bank of Spain
	Cecilia Lozano	Bank of Spain
United Kingdom	Farrukh Nazir	Prudential Regulation Authority
United States	Kirk Odegard	Board of Governors of the Federal Reserve System
	Molly Scherf	Office of the Comptroller of the Currency
	Ann Miner	Federal Reserve Bank of New York
EU	Inge Veldhuis	European Banking Authority (EBA)
Financial Stability Board	Grace Sone	Financial Stability Board
Financial Stability Institute	Amarendra Mohan	Financial Stability Institute
BCBS Secretariat	Motohiro Hatanaka	Secretariat