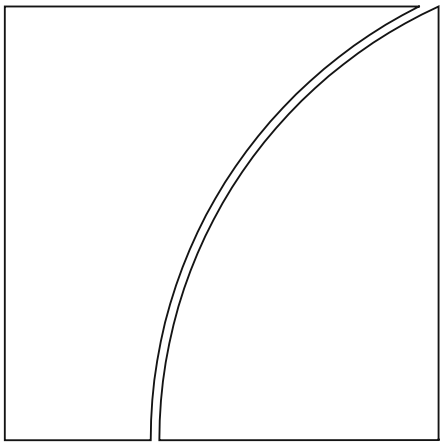
Basel Committee
on Banking Supervision



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

January 2015

BANK FOR INTERNATIONAL SETTLEMENTS

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

ISBN 978-92-9197-035-3 (print)

ISBN 978-92-9197-034-6 (online)

Contents

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

1. Introduction, motivation, methodology

The *Principles for effective risk data aggregation and risk reporting* (the "Principles") were issued by the Basel Committee on Banking Supervision 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 is expected to enhance both their decision-making processes and their resolvability. A complete list of the Principles can be found in Annex 2 of this report.

The Principles are initially applicable 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.

The Basel Committee and national supervisors have 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, which was completed by G-SIBs during 2013.

Taking into consideration the results of the 2013 stocktaking exercise, discussions with the industry, and national supervisors' continuous monitoring of banks, the Basel Committee agreed that it would be appropriate to design a reduced survey and to focus on the fundamentals, particularly: (i) governance; (ii) infrastructure; and (iii) data aggregation accuracy. This report reviews the high-level results of the self-assessment questionnaire.

1.1 Aim of the 2014 bank questionnaire

The questionnaire was intended to establish how each G-SIB views its current compliance status with Principles 1 through 11. The survey enables the supervisory authorities to monitor progress towards full compliance by the 2016 deadline and to help identify and remedy any implementation issues.

[1] The Principles can be found at www.bis.org/publ/bcbs239.htm.

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

1.2 Bank questionnaire scope

To more effectively monitor the progress made in implementing the Principles, a condensed version of the 2013 survey was developed, focusing on the issues considered as essential and/or critical for compliance purposes, or that were related to requirements with weak performance in 2013. The 2013 stocktaking survey included 87 detailed requirements; in comparison, the 2014 survey included 35 questions.[3] Thirty-one G-SIBs and six other large banks (ie non-G-SIBs) participated in the self-assessment exercise.

Among the 35 questions, 11 correspond with the overall Principles, 21 correspond with specific requirements under the Principles, and three additional questions relate to large-scale IT infrastructure projects (Annex 4). Banks were asked to rate their level of compliance with each Principle and requirement. The other 21 questions were included in the 2014 survey because they were noted as being essential for compliance with a given Principle, or had especially weak performance based on the results of the 2013 stocktaking questionnaire. Finally, banks were also asked to provide the expected date of full compliance with each Principle.

The 2014 questionnaire asked for two sets of comments on each question. First, banks were expected to provide general comments. Second, they were asked to describe the impact of any compliance "gap" and potential mitigation tools to be used until they would be able to fully comply with the Principle. Furthermore, banks were expected to explain the potential negative impact or consequences these gaps could have on risk data aggregation and risk reporting capabilities, and, where relevant, what temporary measures will be introduced to mitigate any material issues. The WGSS compared the results from the 2013 stocktaking and the 2014 questionnaire, and set out several recommendations to ensure that banks continue to strive to achieve full compliance by the 2016 deadline.

To assess progress, this report compares the responses of the 30 G-SIBs that participated in the initial 2013 stocktaking with their responses to the 2014 questionnaire.

1.3 Self-assessment rating

In the 2014 questionnaire, banks were requested to rate, on a scale from 1 to 4, their current level of compliance with 11 Principles and 21 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 make further progress 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 expected that if compliance with any one requirement under a Principle was rated below 4, then the general level of compliance with the Principle would also be rated below 4.

[3] Despite the reduced number of questions compared to the 2013 stocktaking, banks are still expected to fully comply with the criteria outlined in the rules text by January 2016.

1.4 Bank questionnaire process

National supervisors administered the questionnaire and banks rated 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 a written assessment of their respective banks' responses. During these interactions, banks and national supervisors discussed:

- Areas where national supervisors thought that ratings might not be accurate,
- Banks' strategy for complying with the Principles; and
- Other comments provided by the banks.

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.

2. Key conclusions from the 2014 Survey

2.1 General conclusions

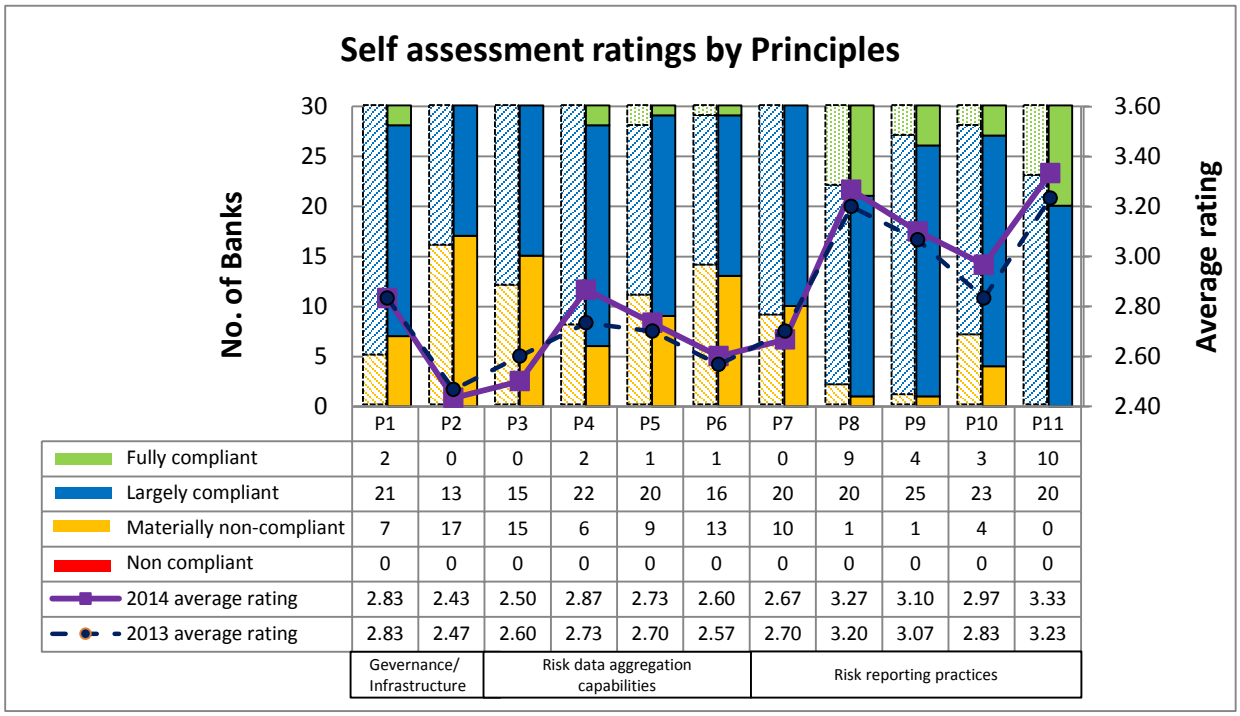
As seen in Graph 1 below, the average ratings of Principles 1 to 11 ranged from 2.43 to 3.33. Overall, there were only minor improvements in average ratings. The three Principles with the lowest reported compliance were Principle 2 (data architecture/IT infrastructure), Principle 6 (adaptability) and Principle 3 (accuracy/integrity) as nearly half of banks reported material non-compliance on these Principles.

The three Principles with the highest reported compliance for both 2013 and 2014 were Principle 8 (comprehensiveness), Principle 9 (clarity/usefulness), and Principle 11 (report distribution).

Compared to the 2013 results, many banks continue to encounter difficulties in establishing strong data aggregation governance, architecture and processes. Banks reported that they often rely on manual workarounds. Similar to the results of the 2013 stocktaking, many firms failed to recognise that governance/infrastructure Principles are important prerequisites for facilitating compliance with the other Principles.[4] As depicted in Graph 1, compliance with Principle 2 (data architecture/IT infrastructure) was rated lowest while Principle 11 (report distribution) was rated highest.

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

Graph 1

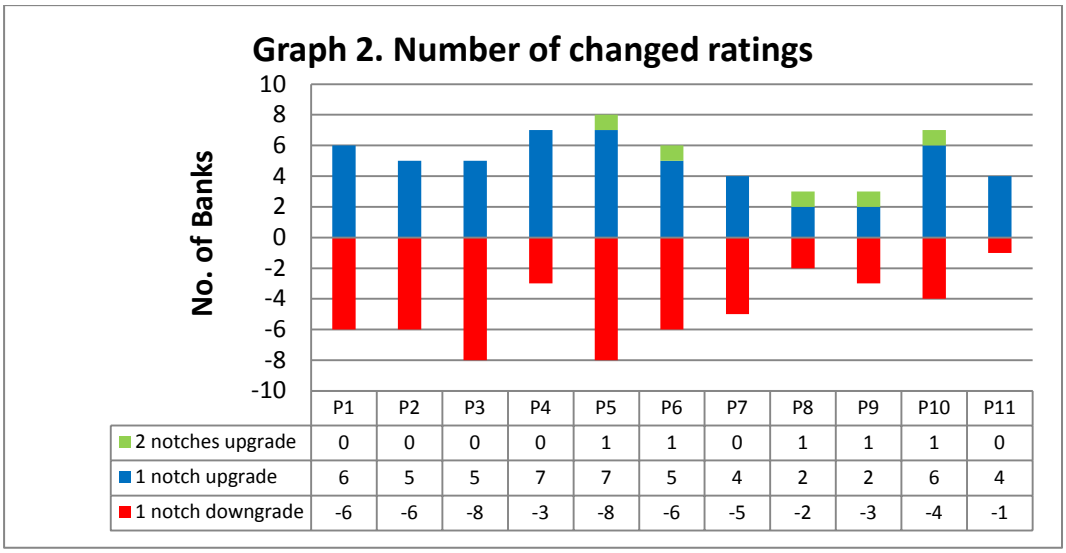


	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11
Fully compliant	2	0	0	2	1	1	0	9	4	3	10
Largely compliant	21	13	15	22	20	16	20	20	25	23	20
Materially non-compliant	7	17	15	6	9	13	10	1	1	4	0
Non compliant	0	0	0	0	0	0	0	0	0	0	0
2014 average rating	2.83	2.43	2.50	2.87	2.73	2.60	2.67	3.27	3.10	2.97	3.33
2013 average rating	2.83	2.47	2.60	2.73	2.70	2.57	2.70	3.20	3.07	2.83	3.23
	Governance/ Infrastructure		Risk data aggregation capabilities				Risk reporting practices				

2.2 Rating changes

Results showed that there were considerable rating changes among the banks, when comparing responses from the 2013 stocktaking with those from the 2014 questionnaire (see Graph 2).

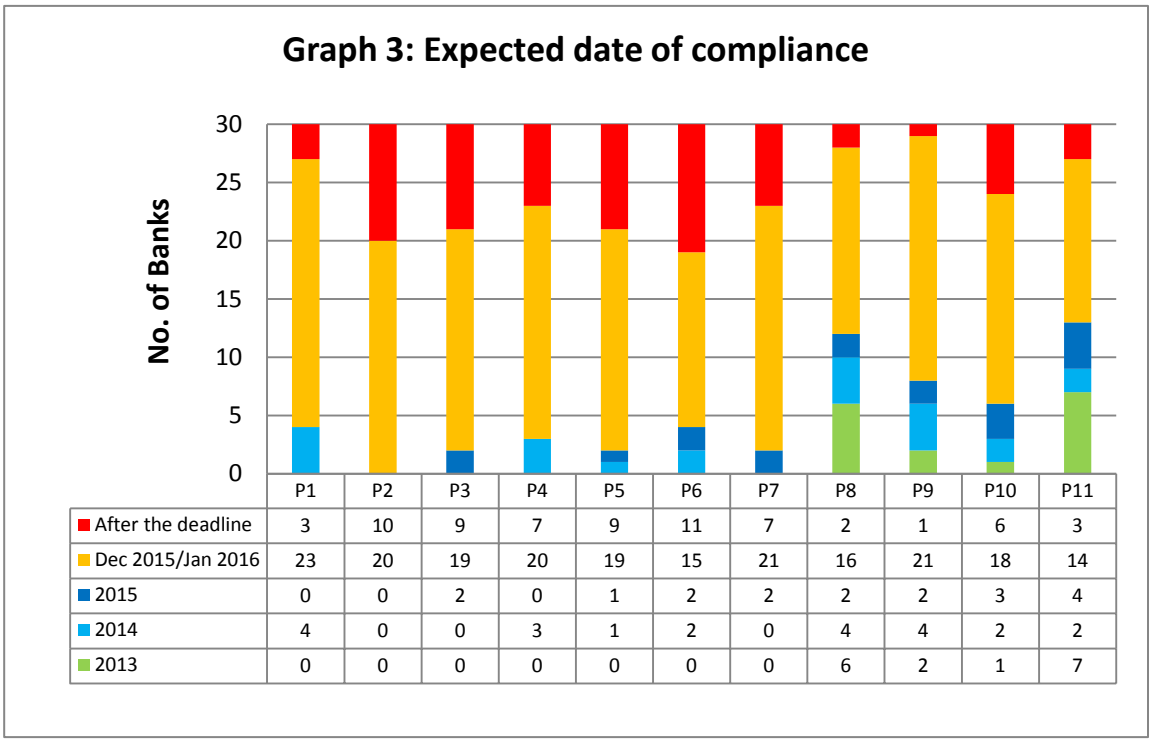
Rating downgrades were reported in at least one Principle by 16 banks. In particular, there were more downgrades in the areas of governance and infrastructure and risk data aggregation capabilities, than in risk reporting. Based on the review of the responses from the banks, there are a number of factors that led to such results. Some banks noted delays in initiating or implementing large-scale IT infrastructure projects as well as the complexity of projects to ensure compliance with the Principles. Importantly, several institutions also noted an improved understanding of the Principles, notably in terms of the scope to be covered (with respect to all material risks and legal entities).



	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11
2 notches upgrade	0	0	0	0	1	1	0	1	1	1	0
1 notch upgrade	6	5	5	7	7	5	4	2	2	6	4
1 notch downgrade	-6	-6	-8	-3	-8	-6	-5	-2	-3	-4	-1

2.3 Expected date of compliance

One of the most noteworthy results of the 2014 questionnaire was that many banks indicated that they will be unable to comply with at least one Principle by the January 2016 deadline. For example, as shown in Graph 3, 11 banks do not anticipate complying with Principle 6 by the January 2016 deadline, and nine banks do not anticipate complying with Principle 3 and Principle 5 by the deadline.



	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11
After the deadline	3	10	9	7	9	11	7	2	1	6	3
Dec 2015/Jan 2016	23	20	19	20	19	15	21	16	21	18	14
2015	0	0	2	0	1	2	2	2	2	3	4
2014	4	0	0	3	1	2	0	4	4	2	2
2013	0	0	0	0	0	0	0	6	2	1	7

In comparison with the results of last year's stocktaking, execution risk appears to have increased. Overall, 14 G-SIBs indicated that they will not fully comply with at least one Principle by the deadline, compared with only 10 banks in the 2013 exercise. Sixteen banks indicated that they plan to

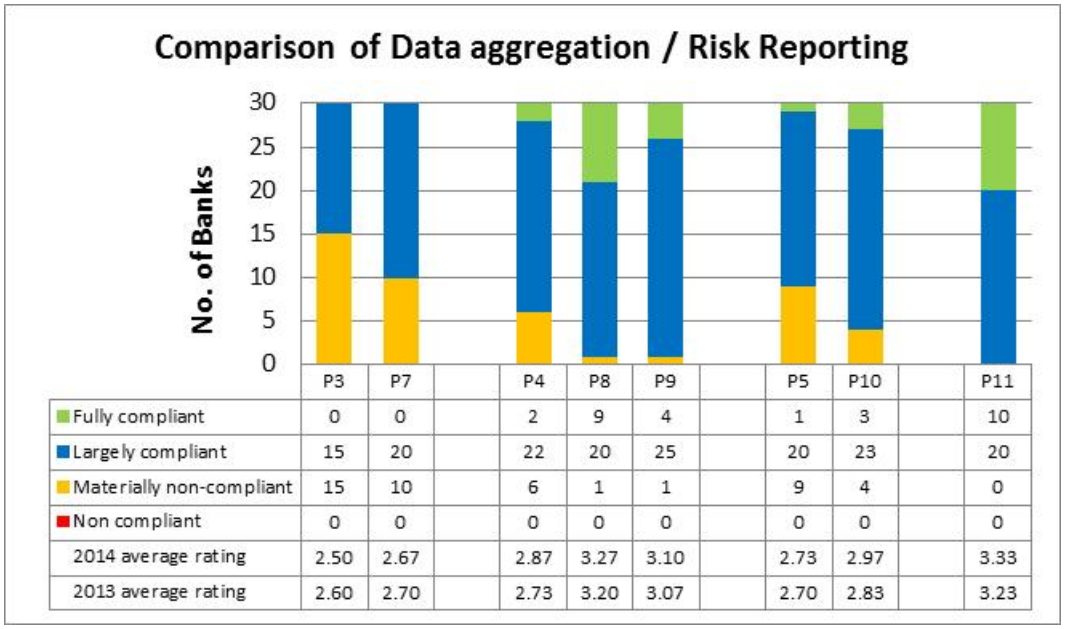
comply with the Principles by the January 2016 deadline. However, given the complexity of ongoing, large-scale data infrastructure projects and noted issues in complying with some of the more fundamental Principles, it appears that banks still have considerable work ahead of them. On a positive note, three banks which expected in 2013 to miss the compliance deadline have now indicated that they expect to meet the deadline. Two additional banks did not report any corresponding rating changes from the 2013 stocktaking to the 2014 questionnaire.

The results of the 2014 questionnaire raise some concern that self-assessments of compliance dates may be overly ambitious. Several G-SIBs that rated themselves as materially non-compliant with several Principles still expected to be compliant by the deadline. For example, 15 G-SIBs rated themselves as materially non-compliant with Principle 3 (data accuracy and integrity), but 10 of those G-SIBs still expected to meet the deadline. Regardless of how the banks rated themselves, anecdotal evidence gathered via the questionnaire suggests that it will be difficult for a number of firms to fully comply with the Principles by 2016.

2.4 Comparison of data aggregation and risk reporting in G-SIBs' self-assessments

Some of the data aggregation and risk-reporting Principles are closely aligned as complying with the former is a prerequisite for complying with the latter. As shown in Graph 4, Principles 3 and 7 address accuracy and integrity in both data aggregation, and reporting. 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.

Graph 4



	P3	P7	P4	P8	P9	P5	P10	P11
Fully compliant	0	0	2	9	4	1	3	10
Largely compliant	15	20	22	20	25	20	23	20
Materially non-compliant	15	10	6	1	1	9	4	0
Non compliant	0	0	0	0	0	0	0	0
2014 average rating	2.50	2.67	2.87	3.27	3.10	2.73	2.97	3.33
2013 average rating	2.60	2.70	2.73	3.20	3.07	2.70	2.83	3.23

*Definition of Principles: P3 = accuracy and integrity; P7 = accuracy; P4 = completeness; P8 = comprehensiveness; P9 = clarity and usefulness; P5 = timeliness; P10 = frequency; P11 = distribution.

However, banks generally assigned themselves higher ratings on the risk-reporting Principles than they did on the related data aggregation Principles. For example, seven banks rated themselves as fully compliant on Principle 8 (comprehensiveness); nevertheless, the same banks rated themselves as largely compliant on Principle 4 (completeness). Those banks considered that risk management reports comprehensively cover all material risk areas, but they indicated the need to enhance the completeness

of risk data aggregation capabilities. Similarly, two banks rated themselves as fully compliant on Principle 10 (frequency) but rated themselves as largely compliant on Principle 5 (timeliness).

2.5 Additional issues regarding strategic IT projects

Finally, as mentioned above, the 2014 survey includes three additional questions related to large-scale IT infrastructure projects. These three questions were added to the survey to obtain a greater understanding of banks' assessment of IT projects that support compliance with the Principles vis-à-vis other projects (see Annex 4 for more details).

Most respondents indicated that they had several IT projects that were intended to support compliance with the Principles. Banks that do not expect to comply with the Principles by January 2016 failed to explain whether it would be possible to ensure that IT projects could be moved to a higher priority. Moreover, the interdependencies associated with large-scale IT projects would make it difficult for banks to re-assign a higher priority to them. Most banks noted that all projects are important, and are funded according to their normal budgeting cycle and are provided with the same level of oversight as other high-priority projects.

2.6 Other large banks' assessments

In addition to G-SIBs, four national supervisors invited six other large banks (ie non-G-SIBs) to complete the questionnaire. However, the sample in the 2014 survey had only four entities in common with the "other large bank" sample in the 2013 exercise.

The compliance levels for non-G-SIBs were similar to those of G-SIBs. None of the non-G-SIB banks rated themselves as non-compliant with any of the Principles, Among the non-G-SIBs, the three Principles with the lowest reported compliance were Principle 2 (data architecture/IT infrastructure), Principle 3 (accuracy and integrity for risk data aggregation) and Principle 7 (accuracy for risk reporting). The Principles for which non G-SIBs reported the highest compliance pertained to risk reporting practices: Principle 8 (comprehensiveness), Principle 9 (clarity and usefulness) and Principle 11 (report distribution). Only three banks expected to comply with all the Principles by the deadline.

2.7 Supervisory plans and recommendations

In comments provided by supervisors, they noted the need for continued supervisory oversight of G-SIBs' progress in closing gaps with the aim of fully complying with the Principles. Supervisors identified the need to meet with bank management and internal audit monitor progress and achieve the necessary oversight. This is deemed critical given the high level of execution risk posed by the fact that many G-SIBs do not expect to be fully compliant prior to the deadline. In order to facilitate implementation, a number of recommendations have been made, including: (i) the need to more fully engage senior management and the board of directors; and (ii) having supervisors more carefully monitor progress on IT architecture projects, the need to minimise use of manual systems, and the importance of quality controls.

3. Governance (Principles 1 and 2)

Table 1

Principle number	Principle	Year	Expected date of full compliance			Number of banks for each rating				
			On or before January 2016	After 2016	Not clear	Rating 1	Rating 2	Rating 3	Rating 4	Average
P1	Governance	2014	**27**	3	0	0	7	21	2	2.83
		2013	29	1	0	0	5	25	0	2.83
P2	Data architecture and IT infrastructure	2014	**20**	9	1	0	17	13	0	**2.43**
		2013	22	8	0	0	16	14	0	2.47

3.1 Quantitative description

G-SIBs reported minimal progress with respect to compliance with Principles 1 (Governance) and 2 (Data and IT infrastructure), which are considered to be prerequisites for overall compliance with RDARR Principles. Consistent with 2013 results, the G-SIBs identified Principle 2 as the most challenging, as it attracted the lowest average compliance rating, of 2.43.

Only two G-SIBs reported compliance with the Governance Principle, and no G-SIBs fully comply with the Data Architecture and IT Infrastructure Principle. Of particular note, six G-SIBs downgraded their ratings for each of these Principles as compared with their self-assessment ratings from 2013 to 2014.

The majority of G-SIBs (70%) rated themselves as "3" (materially compliant) with the Governance Principle, while fewer than half (43%) rated themselves materially compliant with the data architecture and IT infrastructure Principle.

Seven G-SIBs rated themselves "2", (materially non-compliant or needing significant actions to meet the requirement) for the Governance Principle, and more than half of the G-SIBs (57%) rated themselves a "2" for the data architecture and IT infrastructure Principle.

Several G-SIBS reported that they do not expect to achieve full compliance with these two Principles by the January 2016 deadline. In fact, the number of G-SIBs expected to miss the deadline for compliance has increased since 2013. At least nine G-SIBs do not expect to meet Principle 2 by January 2016, and three do not expect to meet Principle 1 by January 2016 (compared to eight and one, respectively, in 2013).

3.2 Challenges

The most common weaknesses identified by G-SIBs were: (i) the need to continue expanding components of an enterprise-wide governance framework and (ii) to manage multiple large-scale projects related to RDARR. Many banks continue to point to the need to enhance current IT architecture and data flows to reduce complexity and manual workarounds. Frequently, G-SIBs commented that IT infrastructure, while adequate in normal times, was not adequate in stress or crisis situations.

While many banks have most elements of a governance framework, particular elements (by risk type or across legal jurisdictions) were noted as requiring additional policies, procedures and controls. G-SIBs noted enhanced data quality standards, manual workarounds, and appropriate governance as current processes for mitigating potential exposures until the necessary IT architecture is fully established.

3.3 Potential strategies for compliance

In order to meet the requirements of the Governance Principle, G-SIBs reported they will continue to define and clarify the functions and roles required under enterprise-wide data governance. G-SIBs noted that additional work was necessary on cross-functional implementation initiatives involving risk, compliance, IT, finance and internal control functions.

Further enhancements are planned to risk reports with a view to providing metrics on limitations (eg data quality, completeness) for a better understanding of data quality and to provide further assurance around the underlying processes. Escalation processes when outside tolerances also need to be implemented at certain G-SIBs.

It was indicated that improvements to board-level reporting are a necessary action step. For some banks, the current limitations of risk reporting have yet to be communicated to the board. Increased transparency and or expanded narrative descriptions are other planned action items. While the above actions involve reporting, it is noteworthy that governance processes for escalation and description of current limitations are not in place at reporting G-SIBs.

With respect to data architecture and IT infrastructure, G-SIBs report the following needed action steps:

- Improving IT infrastructure so that more frequent data are available for certain risk areas (credit risk and liquidity risk);
- Process improvements to infrastructure so as to reduce reliance on manual workarounds and to automate aggregations;
- Simplifying current IT architecture and data flows across departments and legal entities to streamline the aggregation process and to enable quick aggregation of risk data during times of stress;
- Ensuring that consistent and integrated data taxonomies and dictionaries exist at the group level, and throughout the organisation; and
- Identifying and defining "data owners" to improve accountability.

As depicted in Table 1, three G-SIBs do not expect to meet Principle 1, and at least nine (possibly 10) G-SIBs do not expect to comply with Principle 2 by the January 2016 deadline. In some cases, G-SIBs reported that appropriate communication would be made to the board of directors on progress.

For some G-SIBs, infrastructure solutions will span multiple years beyond the deadline. Respondents stated that an adequate governance framework and documentation would be in place, and would mitigate any potential negative effects or outcomes until the infrastructure solutions are in place.

For the nine (possibly 10) G-SIBs indicating that they would not be able to meet the deadline, none anticipated a material negative impact of compliance gaps on risk management decisions. To address compliance gaps with this Principle, the G-SIBs intend to:

- Rely on manual workarounds with appropriate controls and expert judgement;
- Establish data governance frameworks including data quality standards; and

- Prioritise high-impact risk data items in the remediation process.

4. Data aggregation (Principles 3, 4, 5 and 6)

Table 2

Principle number	Principle	Year	Expected date of full compliance			Number of banks for each rating				
			On or before January 2016	After 2016	Not clear	Rating 1	Rating 2	Rating 3	Rating 4	Average
P3	Accuracy and integrity	2014	**21**	8	1	0	15	15	0	**2.50**
		2013	26	4	0	0	12	18	0	2.60
P4	Completeness	2014	**23**	6	1	0	6	22	2	2.87
		2013	24	6	0	0	8	22	0	2.73
P5	Timeliness	2014	**21**	8	1	0	9	20	1	2.73
		2013	26	4	0	0	11	17	2	2.70
P6	Adaptability	2014	**19**	10	1	0	13	16	1	2.60
		2013	25	5	0	0	14	15	1	2.57

4.1 Quantitative description

In the area of risk data aggregation, G-SIBs' average self-assessment compliance ratings improved from 2013 with respect to most RDARR Principles (Table 2). The notable exception was Principle 3 (accuracy and integrity), for which banks' ratings are evenly split between "materially non-compliant" and "largely compliant". The overall deterioration in the average compliance rating for Principle 3 is the result of several institutions downgrading their ratings due to delays in certain projects as well as a greater understanding of the scope of the risks covered in the Principle. Such a trend is all the more noteworthy since, in the area of risk data aggregation capabilities, a relatively large number of requirements for Principle 3 that were considered as being "essential" for complying with the Principle as well as requirements where performance was weak based on the results of the 2013 stocktaking. In this respect, the level of compliance remains particularly low, at around 2.5, for requirements 12 (there is an appropriate balance between automated and manual systems) and 13 (proper documentation of risk data aggregation processes).

In contrast with Principle 3, the average compliance rating for Principle 4 (completeness) improved, with nearly two thirds of the respondents considering their practices as being "largely compliant". Requirement 15, an essential element for compliance under Principle 4, states that banks should include all material risk data in banks' data aggregation capabilities. The requirement registers a satisfactory average level of compliance, of 3.1.

Regarding the expected date of full compliance, the number of G-SIBs indicating that they will not be in a position to comply by January 2016 doubled with respect to Principle 3 (accuracy and integrity), Principle 5 (timeliness) and Principle 6 (adaptability). Slightly less than one third of all respondents expect that they will not be compliant with Principles 3, 5 and 6 by January 2016.

4.2 Challenges

G-SIBs reported five key challenges to compliance with the Principles in the area of risk data aggregation.

First, consistent with the results of 2013 stocktaking, G-SIBs have a heavy reliance on manual processes and interventions to create risk reports. While market risk data (and to some extent, liquidity risk data) are largely automated, manual processes are still widely used in many risk areas and across businesses and functions. This impedes banks in generating ad hoc data report requests in a timely and accurate manner, especially in times of stress or crisis situations. In this context, G-SIBs pointed out the importance of enhancing their IT infrastructures to support daily data aggregation in situations of stress/crisis. Some of them also underlined the need to improve their production of risk information and metrics (notably in domains other than market risk) on a timely basis to meet all risk management requirements.

Second, G-SIBs appear unable to consistently and comprehensively document risk data aggregation processes at the group level, including clearly defining material risk across business lines and legal entities. A possible solution to this issue is the implementation of formal "data dictionaries" consistently covering all risk categories at the group level, thus reducing the time required to generate customised reports. The development of an End User Computing Policy (EUC) would help capture and ensure complete documentation of all material manual processes at the group level.

Third, G-SIBs reported difficulties improving their ability to aggregate collateral-related data for derivatives transactions. G-SIBs also noted the challenges in aggregating off-balance sheet risk data, due, in part, to the non-linearity of the measures and the lack of harmonisation across jurisdictions.

Fourth, G-SIBs reported difficulties in establishing adequate automated reconciliation processes for risk data aggregation, notably for managerial risk data with regulatory and/or accounting data. More broadly, throughout the reconciliation process, banks are striving to address the key challenge of ensuring a consistent level of granularity of information and sufficient documentation of material discrepancies across source systems.

Finally, several G-SIBs highlighted that legal restrictions in some regions/countries have hindered them in producing a granular level of details on risk data.

4.3 Potential strategies for compliance

To address the challenges relating to the compliance with the Principles and associated requirements in the area of risk data aggregation, reported action items included:

- Developing IT infrastructure to aggregate a broader range of risk data automatically and reduce reliance on manual workarounds;
- Automating data quality controls and improving reporting capabilities associated with group-wide stress testing;
- Improving systems to monitor and enforce credit limits status across risk types and products;
- Promoting data alignment between risk and finance, using common data dictionaries and appropriate governance structure;
- Establishing data collection channels, processes and procedures that encompass the development of common taxonomies and reference data so as to facilitate data aggregation in times of stress/crisis;
- Enhancing data aggregation capabilities to consolidate data from branches and subsidiaries operating in other jurisdictions and, more generally, developing consolidated data stores,

notably for credit, market and operational risks to expedite risk reporting and easier reconciliation of risk data;

- Implementing programmes aimed at meeting Basel III regulatory requirements and other international initiatives (eg Legal Entity Identifiers); and
- Providing appropriate access to sufficient staff with expert knowledge of risk control functions and data so they are able to process ad-hoc data report requests.

5. Risk reporting (Principles 7, 8, 9, 10 and 11)

Table 3

Principle number	Principle	Year	Expected date of full compliance			Number of banks for each rating				
			On or before January 2016	After 2016	Not clear	Rating 1	Rating 2	Rating 3	Rating 4	Average
		2014	**23**	7	0	0	10	20	0	**2.67**
P7	Accuracy	2013	26	4	0	0	9	21	0	2.70
		2014	28	2	0	0	1	20	9	3.27
P8	Comprehensiveness	2013	28	2	0	0	2	20	8	3.20
		2014	29	1	0	0	1	25	4	3.10
P9	Clarity and usefulness	2013	29	1	0	0	1	26	3	3.07
		2014	**24**	5	1	0	4	23	3	2.97
P10	Frequency	2013	26	4	0	0	7	21	2	2.83
		2014	**27**	3	0	0	0	20	10	3.33
P11	Distribution	2013	29	1	0	0	0	23	7	3.23

5.1 Quantitative description

For the Principles relating to risk reporting, the results of the 2014 questionnaire were fairly similar to the results of the 2013 stocktaking exercise. G-SIBs generally assigned themselves higher ratings on the risk-reporting Principles than they did on the corresponding data aggregation Principles. As in the 2013 survey, the average reported level of compliance for Principle 11 (distribution) on the 2014 survey is the highest among all the Principles (Table 3). The average compliance from 2013 to 2014 slightly increased for Principle 8 (comprehensiveness), Principle 9 (clarity and usefulness), Principle 10 (frequency), and Principle 11. Among the Principles for risk reporting, only Principle 7 (accuracy) saw an overall deterioration in ratings from 2013 to 2014, from 2.70 to 2.67.

At least 27 banks expect to comply with Principle 8, Principle 9 and Principle 11 by the January 2016 deadline. Fewer banks expect to comply with Principle 7 (23 G-SIBs) and Principle 10 (24 G-SIBs) by the deadline. For Principles 7, 10, and 11, the number of G-SIBs indicating that they would comply by the deadline slightly decreased in comparison with the 2013 stocktaking. For Principles 8 and 9, the number of G-SIBs indicating they would comply by January 2016 remained the same from 2013 to 2014.

5.2 Challenges

The primary challenges G-SIBs face in this area are similar to the challenges in complying with other Principles. This highlights the interdependencies among the Principles, and underscores that compliance with some of the more fundamental Principles will facilitate compliance with the risk-reporting Principles. For Principle 7 (accuracy), the G-SIBs first and foremost identified the difficulty in developing consistent approaches for producing accurate manually generated reports in cases where automated reports cannot be produced. The banks noted that issues related to the accuracy of reports are exacerbated during stressful periods. The banks also noted that the frequency of reports also suffers during stressed or crisis situations.

Most of the respondents maintained that their risk reports cover all material risk areas within their organisations and that the scope and depth of the reporting are consistent with the banks' complexity, size and risk. The banks did not note any particularly overwhelming issues with Principle 8 (comprehensiveness) in terms of establishing appropriate internal policies and procedures to create comprehensive reports. The more challenging issue is in the consistent monitoring of these reports to ensure that they remain appropriately comprehensive given changes in reporting metrics or in ensuring that reports are available on both single-line (legal, business, particular risks etc) and aggregate/consolidated levels. In addition, the overarching issue of developing appropriately comprehensive reports during stressed or crisis situations was raised.

For Principle 9, (clarity and usefulness), the banks noted a number of challenges in establishing a common terminology within reports for management. The banks cited non-existent or incomplete data dictionaries, inconsistent metadata fields, and non-integrated data taxonomies as barriers to complying with Principle 9.

The respondents cited a number of issues regarding the development of appropriately frequent reports (Principle 10) to board and senior management given the nature of the risk or situation. In general, respondents noted that there is often a trade-off between speed and accuracy/comprehensiveness in reporting, particularly for manually created reports. The banks noted that existing information technology infrastructure cannot create daily aggregation reports, as some financial data are not available on a daily basis. As stated previously with Principle 7, manually generated reports also present challenges in complying with Principle 10. More specifically, resource-intensive manual processes make it difficult to quickly provide senior management with various risk reports, particularly those on liquidity, wholesale credit risk, and other critical credit positions and exposures.

In terms of distributing risk management reports (Principle 11) the banks did not greatly elaborate on the challenges and issues because many already have procedures in place for distributing reports to senior management and the board of directors, as appropriate, while adhering to the information security and confidentiality Principles. However, banks stated that some challenges exist in complying with this Principle and ensuring a sufficiently robust reporting distribution, particularly during stress and crisis situations.

5.3 Potential strategies for compliance

Most banks indicated that existing risk management report processes cover material risk areas and that the scope and depth of reporting is consistent with their complexity, size and risk profile. In addition, banks noted that they have procedures in place for report distribution with appropriate security practices.

Nevertheless, the G-SIBs identified a number of possible action items to help move towards compliance with the risk reporting Principles. In terms of improving report accuracy (Principle 7), some G-SIBs noted the importance of:

- Developing procedures, policies, and controls to produce documents and ensure their accuracy and clarity for both regular and crisis reporting along with implementing reasonableness checks and identification of errors or weaknesses.
- Improving board and senior management communication of data errors and weaknesses in risk reporting.

To address the challenges in developing clear and useful reports (Principle 9) a number of institutions noted the need to continue developing standard terms, glossaries or data dictionaries, focusing on concepts such as taxonomy, data classification, and metadata as a part of the authorised data source structure. G-SIBs also noted the significance of periodically reviewing reports to verify data quality so that they meet the needs of senior management.

To improve the frequency of risk data reporting (Principle 10), a number of G-SIBs are in the process of making large-scale IT improvements such as data warehouses, which will allow for faster capital markets risk reporting and facilitate the reconciliation of finance and risk data. Such IT improvements are typically developed at the consolidated or holding company level to support the automated aggregation of credit risk and liquidity risk data. Moreover, the development of IT infrastructure at the consolidated/aggregate level will typically enhance firms' ability to systematically aggregate exposure across disparate systems. Other high-level initiatives that firms are undertaking to improve the frequency of risk data reporting include establishing data management offices and improving data interfaces/databases in the course of completing large-scale IT projects.

Most of the firms noted that risk management reports are distributed (Principle 11) to the relevant recipients with the appropriate controls over security and confidentiality. Several firms noted the need to:

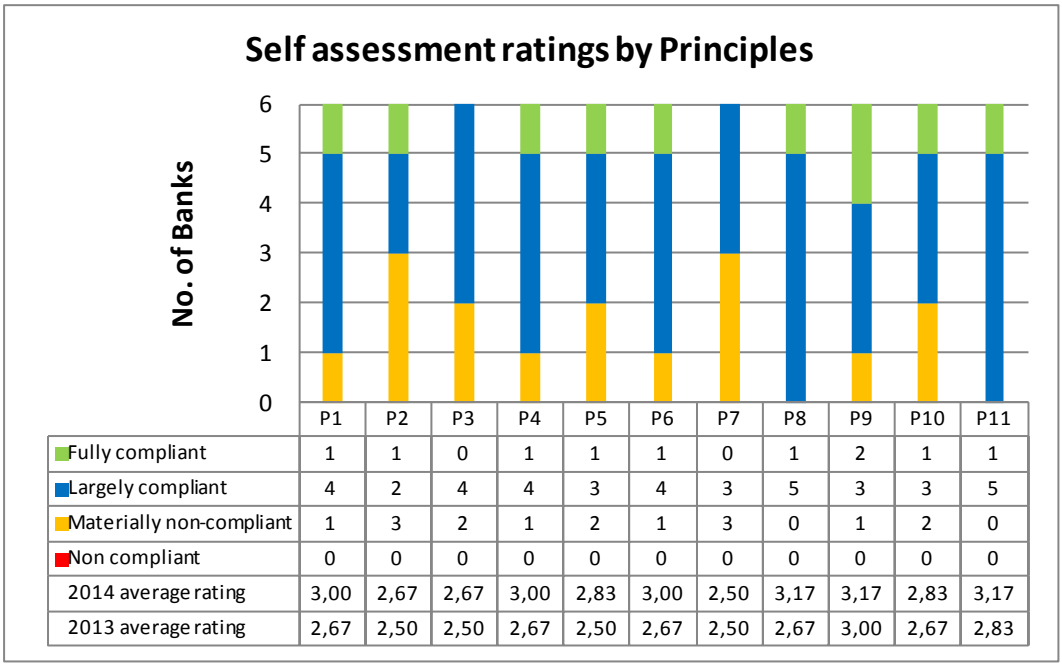
- Develop or enhance the governance and documentation of distribution procedures and data confidentiality arrangements;
- Implement additional report access controls across risk types with regards to report viewing and distribution; and
- Create information security policies for the distribution of management reports, which includes the use of secured media such as collaborative workspaces and encrypted e-mails.

6. Self-assessments by other large banks

As in 2013, Basel Committee member jurisdictions were invited to include other large banks (ie non-G-SIBs) in the exercise. In 2014, this sample included six other large banks from four countries. Taking into account the limited sample, these six banks may not be representative of all other large banks.

In addition the sample is not the same as in the 2013 exercise (having only four banks in common) and it is therefore difficult to assess year-by-year progress towards full compliance by 2016 in this section. As seen in Graph 5, no bank rated itself as non-compliant with any of the Principles. The three Principles with the lowest reported compliance were Principle 2 (data architecture/IT infrastructure), Principle 3 (accuracy and integrity for risk data aggregation) and P7 (accuracy for risk reporting). Half of the banks rated themselves as materially non-compliant on Principles 2 and 7. The Principles for which banks reported the highest compliance pertained to reporting: Principles 8 (comprehensiveness), 9 (clarity and usefulness) and 11 (report distribution). Only three banks expected to comply with the all the Principles by January 2016 or before.

Graph 5



	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11
Fully compliant	1	1	0	1	1	1	0	1	2	1	1
Largely compliant	4	2	4	4	3	4	3	5	3	3	5
Materially non-compliant	1	3	2	1	2	1	3	0	1	2	0
Non compliant	0	0	0	0	0	0	0	0	0	0	0
2014 average rating	3,00	2,67	2,67	3,00	2,83	3,00	2,50	3,17	3,17	2,83	3,17
2013 average rating	2,67	2,50	2,50	2,67	2,50	2,67	2,50	2,67	3,00	2,67	2,83

7. Discussions with industry

In a similar exercise after the 2013 stocktaking, the WGSS engaged in an industry discussion regarding the some of the preliminary results of the 2014 survey. The industry provided a number of explanations regarding the number of ratings changes, both upgrades and downgrades, from 2013. They mentioned that despite the numerous quantitative ratings downgrades, there has been progress in complying with the RDARR Principles. Industry representative stated that their boards of directors and senior management are acutely aware of the importance of RDARR, and that there is generally a higher level of understanding of the Principles. They also maintain that effective RDARR is an ongoing process and that there is much work to be done to comply with the Principles by the January 2016 and beyond.

In terms of the challenges that banks face in attempting to comply with the Principles, the industry panel indicated that the completion of large-scale IT infrastructure projects will aid in complying with the Principles. However, large scale IT projects are dependent on many smaller dependent IT projects, which increases execution risk. Also contributing to execution risk is the lack of subject matter experts to improve RDARR processes. Moreover they indicated the changing regulatory landscape, and consequent required reporting, further complicates the execution of IT projects. Industry members noted that the completion of these projects will improve business-as-usual RDARR, which will improve, but not completely resolve, challenges in risk reporting during periods of stress. Among the greatest challenges in risk reporting during periods of stress is the over-reliance of manually-created reports and developing processes and procedures for developing such reports when automated reports cannot be developed.

8. Supervisory assessment

Based on their knowledge of participating G-SIBs, supervisors indicated that the questionnaire results broadly reflect the current state of implementation. They also found the ratings to be generally credible, and consistent with their understanding of the G-SIBs' data aggregation and reporting capabilities.

Nevertheless, 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 may have been interpreted inconsistently across banks. In addition, although national supervisors reviewed responses and discussed them with banks in their jurisdictions much more thoroughly in 2014 than in the 2013 stocktaking, they were not asked to validate the accuracy of the ratings or comments, nor did they assess the potential differences in the level of rigour applied by each bank or the differences in home/host supervisory approaches.

Through their responses, the banks demonstrated that they understand the importance of the Principles and are committed to enhancing their risk data aggregation and risk-reporting capabilities. In comparison with the 2013 stocktaking, the G-SIBs noted a number of ratings increases and decreases for most of the Principles in the 2014 survey. It is possible that the number of downgrades that banks reported for various Principles highlighted the banks' growing understanding of the Principles and the challenges that remain in complying with them. Based on the review of the qualitative responses to many of the 2014 survey questions, it appears the G-SIBs have extensive work to do before they can comply with some of the RDARR Principles, principally those covering governance and data aggregation.

Regarding the compliance date, the results of the 2014 questionnaire raise some concerns that banks intending to comply by the January 2016 deadline may be overly ambitious. For instance, several G-SIBs have rated themselves as materially non-compliant with several Principles, yet expect to comply by the January 2016 deadline. More specifically, 15 G-SIBs rated themselves as materially non-compliant with Principle 3; however, 10 of those G-SIBs expect to meet the deadline. Given the complexity of large-scale IT infrastructure projects, it may be difficult for some banks to achieve compliance by 2016. Regardless of how the banks rated themselves in the 2014 questionnaire (materially non-compliant or otherwise), it would appear that a number of firms will find it difficult to fully comply with the Principles by 2016, judging from a review of the work that remains to be done.

G-SIBs generally assigned themselves higher ratings for the Principles relating to risk reporting than they did on those relating to data aggregation or governance. While the banks may have adequate processes and procedures in place for report distribution, they may be overstating their level of compliance. This is particularly true given their continued reliance on manually produced reports, particularly in stressed or crisis situations, as well as for assessing emerging risks. It is still questionable how reliable and useful these banks risk reports can be when the data within these reports and the procedures and processes to produce them are in need of improvements.

Results showed that there remain some significant common challenges to full compliance with the Principles:

- Banks' dependence on manual processes;
- The need to develop common data dictionaries and data taxonomies; and
- The inability to create accurate and timely risk data reports during stressed or crisis situations.

Notwithstanding this, many G-SIBs stated that they do not anticipate any material negative impact from compliance gaps, or they maintain that their manual processes are adequate stop-gaps.

9. Conclusion: supervisory plans and recommendations

Supervisory authorities have indicated that they have a variety of supervisory tools ranging from information-gathering powers to the enforcement of penalties and capital add-ons if their regulated G-SIBs or D-SIBs fail to comply with the Principles. However, a number of supervisory authorities indicated that the application of specific tools depends on the nature of the issue and its impact on supervisory objectives. There is no uniform strategy among authorities for applying any specific tool, and their

responses indicated that they are likely to follow a risk-based assessment of compliance with the Principles to determine the most appropriate supervisory tools to apply.

Based on the results noted above, the WGSS has six recommendations for supervisors to support the timely implementation of the Principles. Furthermore, it is suggested that these recommendations be published as part of the public report (Annex 2).

1. Supervisory authorities which have not yet introduced any changes to the broader supervisory framework to implement the Principles should consider the feasibility of introducing such changes. Those supervisory authorities who share a common regulatory framework with regional supranational authorities should introduce common guidance.

2. Supervisory authorities regulating D-SIBs which have not yet engaged with their D-SIBs should enter into initial discussions to assess how their D-SIBs will implement the Principles within the three-year time frame after they are designated as D-SIBs.

3. Supervisory authorities should ensure that the banks' senior management and boards of directors are directly involved in assessing progress in implementation, as well as in identifying and enabling timely resolution of any obstacles to full implementation by 2016.

4. Supervisory authorities should leverage the self-assessment questionnaire, as well as the results and other information provided by the WGSS, to enhance their oversight of progress in implementation. This could involve, among other things, conducting their own assessments of progress, using the WGSS survey questions as a template. Likewise, supervisors could use the results to benchmark progress or conduct peer comparisons.

5. The results of the banks' self-assessments have not been validated by supervisors. However, supervisory authorities should not wait until the implementation deadline to review the results, build assessments of their validity into supervisory programmes, and take action as needed to enable timely implementation. Supervisory authorities should review the results of the bank self-assessment survey in developing strategies to assess progress, in particular, large year-over-year changes for individual banks. Finally, given the results of the self-assessment and discussions with industry, the following three topics should be discussed in depth:

   (a) Timely implementation of IT architecture, as well as banks' tactical mitigants while longer-term strategic solutions are being developed;

   (b) The desired balance between automated and manual systems; and

   (c) Quality controls in place.

6. Finally, supervisory authorities should continue to actively exchange information on how they intend to facilitate compliance, or remedy non-compliance.

Annex 1: 31 G-SIBs participating in the 2014 survey[5,6]

Jurisdiction	G-SIBs
China	Bank of China Industrial and Commercial Bank of China Limited
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

[5] Dexia is undergoing an orderly resolution process and did not participate in this survey.

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

Annex 2: List of 11 Principles and 35 requirements in 2014 survey[7]

	Principles		Requirements
Governance/infrastructure	1. Governance	1	Framework established
		2	Approval of the Framework and resources deployed
		3	Full documentation and validation
		4	Board's awareness of limitations
		5	Overall assessment and expected date of full compliance
	2. Data architecture & IT infrastructure	6	Data taxonomies*
		7	Adequate controls through the lifecycle of data
		8	Overall assessment and expected date of full compliance
Risk data aggregation capabilities	3. Accuracy and integrity	9	Mitigants and controls for manual processes
		10	Reconciliation with different sources
		11	Dictionary
		12	Balance between automated and manual systems*
		13	Documentation of risk data aggregation processes*
		14	Overall assessment and expected date of full compliance
	4. Completeness	15	All material risk data included
		16	Overall assessment and expected date of full compliance
	5. Timeliness	17	Capabilities to produce timely information to meet reporting requirements
		18	Overall assessment and expected date of full compliance
	6. Adaptability	19	Customisation of data
		20	Overall assessment and expected date of full compliance
Risk reporting practices	7. Accuracy	21	Automated and manual edit and reasonableness checks
		22	Integrated procedure identifying data errors and reporting
		23	Accuracy requirements for regular and stress cases*
		24	Overall assessment and expected date of full compliance
	8. Comprehensiveness	25	Reporting in line with business model and risk profile
		26	Overall assessment and expected date of full compliance
	9. Clarity and usefulness	27	Inventory and classification of risk data items
		28	Overall assessment and expected date of full compliance
	10. Frequency	29	Availability of all critical exposure reports shortly in stress situations
		30	Overall assessment and expected date of full compliance
	11. Distribution	31	Timely dissemination of reports balanced with appropriate confidentiality
		32	Overall assessment and expected date of full compliance
IT projects		33	Strategic priority of data/IT projects
		34	Ability to reschedule projects if not completed by 2016
		35	Oversight of progress

[7] Indicates that the requirement was one of the lowest scores in 2013 AND was deemed an essential requirement.

Annex 3: Average ratings sort by P1 to P11

2014 No.	2013 No.	Brief explanation of each requirement	2014 Self assessements									2013 Self assessements									Changes								
			No. of banks for each rating				Average rating	% for each rating				No. of banks for each rating				Average rating	% for each rating				No. of banks for each rating				Average rating	% for each rating			
			1 NC	2 MNC	3 LC	4 FC		1	2	3	4	1 NC	2 MNC	3 LC	4 FC		1	2	3	4	1 NC	2 MNC	3 LC	4 FC		1	2	3	4
R1	R1	Framework established	0	4	22	4	3.00	0%	13%	73%	13%	0	8	19	3	2.83	0%	27%	63%	10%	0	-4	+3	+1	+0.17	0%	-13%	+10%	+3%
R2	R2	Approval of the framework and resources deployed	0	12	15	3	2.70	0%	40%	50%	10%	0	16	12	2	2.53	0%	53%	40%	7%	0	-4	+3	+1	+0.17	0%	-13%	+10%	+3%
R3	R5	Full documentation and validation	0	9	19	2	2.77	0%	30%	63%	7%	0	13	16	1	2.60	0%	43%	53%	3%	0	-4	+3	+1	+0.17	0%	-13%	+10%	+3%
R4	R14	Board's awareness of limitations	0	7	16	7	3.00	0%	23%	53%	23%	0	5	19	6	3.03	0%	17%	63%	20%	0	+2	-3	+1	-0.03	0%	+7%	-10%	+3%
P1	**P1**	**GOVERNANCE**	**0**	**7**	**21**	**2**	**2.83**	**0%**	**23%**	**70%**	**7%**	**0**	**5**	**25**	**0**	**2.83**	**0%**	**17%**	**83%**	**0%**	**0**	**+2**	**-4**	**+2**	**+0.00**	**0%**	**+7%**	**-13%**	**+7%**
R6	R19	Data taxonomies	1	23	6	0	2.17	3%	77%	20%	0%	0	20	9	1	2.37	0%	67%	30%	3%	+1	+3	-3	-1	-0.20	+3%	+10%	-10%	-3%
R7	R22	Adequate controls through the life cycle of data	0	12	16	2	2.67	0%	40%	53%	7%	0	14	14	2	2.60	0%	47%	47%	7%	0	-2	+2	0	+0.07	0%	-7%	+7%	0%
P2	**P2**	**DATA ARCHITECTURE AND IT INFRASTRUCTURE**	**0**	**17**	**13**	**0**	**2.43**	**0%**	**57%**	**43%**	**0%**	**0**	**16**	**14**	**0**	**2.47**	**0%**	**53%**	**47%**	**0%**	**0**	**+1**	**-1**	**0**	**-0.03**	**0%**	**+3%**	**-3%**	**0%**
R9	R26	Mitigants and controls for manual processes	0	12	13	5	2.77	0%	40%	43%	17%	0	11	14	5	2.80	0%	37%	47%	17%	0	+1	-1	0	-0.03	0%	+3%	-3%	0%
R10	R27	Reconciliation with different sources	0	7	19	4	2.90	0%	23%	63%	13%	0	7	20	3	2.87	0%	23%	67%	10%	0	0	-1	+1	+0.03	0%	0%	-3%	+3%
R11	R29	Dictionary	0	14	14	2	2.60	0%	47%	47%	7%	0	13	15	2	2.63	0%	43%	50%	7%	0	+1	-1	0	-0.03	0%	+3%	-3%	0%
R12	R30	Balance between automated and manual systems	0	18	11	1	2.43	0%	60%	37%	3%	0	18	10	2	2.47	0%	60%	33%	7%	0	0	+1	-1	-0.03	0%	0%	+3%	-3%
R13	R31	Documentation of risk data aggregation process	0	17	13	0	2.43	0%	57%	43%	0%	0	17	13	0	2.43	0%	57%	43%	0%	0	0	0	0	0.00	0%	0%	0%	0%
P3	**P3**	**ACCURACY AND INTEGRITY**	**0**	**15**	**15**	**0**	**2.50**	**0%**	**50%**	**50%**	**0%**	**0**	**12**	**18**	**0**	**2.60**	**0%**	**40%**	**60%**	**0%**	**0**	**+3**	**-3**	**0**	**-0.10**	**0%**	**+10%**	**-10%**	**+0%**
R15	R38	All material risk data included	0	4	19	7	3.10	0%	13%	63%	23%	0	4	19	7	3.10	0%	13%	63%	23%	0	0	0	0	0.00	0%	0%	0%	0%
P4	**P4**	**COMPLETENESS**	**0**	**6**	**22**	**2**	**2.87**	**0%**	**20%**	**73%**	**7%**	**0**	**8**	**22**	**0**	**2.73**	**0%**	**27%**	**73%**	**0%**	**0**	**-2**	**0**	**+2**	**+0.13**	**0%**	**-7%**	**+0%**	**+7%**
R17	R46	Capabilities to produce timely information to meet reporting requirements	0	9	20	1	2.73	0%	30%	67%	3%	0	9	19	2	2.77	0%	30%	63%	7%	0	0	+1	-1	-0.03	0%	0%	+3%	-3%
P5	**P5**	**TIMELINESS**	**0**	**9**	**20**	**1**	**2.73**	**0%**	**30%**	**67%**	**3%**	**0**	**11**	**17**	**2**	**2.70**	**0%**	**37%**	**57%**	**7%**	**0**	**-2**	**+3**	**-1**	**+0.03**	**0%**	**-7%**	**+10%**	**-3%**
R19	R51	Customization of data	0	13	16	1	2.60	0%	43%	53%	3%	0	14	15	1	2.57	0%	47%	50%	3%	0	-1	+1	0	+0.03	0%	-3%	+3%	0%
P6	**P6**	**ADAPTABILITY**	**0**	**13**	**16**	**1**	**2.60**	**0%**	**43%**	**53%**	**3%**	**0**	**14**	**15**	**1**	**2.57**	**0%**	**47%**	**50%**	**3%**	**0**	**-1**	**+1**	**0**	**+0.03**	**0%**	**-3%**	**+3%**	**0%**
R21	R57	Automated and manual edit and reasonableness checks	0	14	15	1	2.57	0%	47%	50%	3%	0	14	14	2	2.60	0%	47%	47%	7%	0	0	+1	-1	-0.03	0%	0%	+3%	-3%
R22	R58	Integrated procedure for identifying and reporting data errors	0	11	17	2	2.70	0%	37%	57%	7%	0	14	14	2	2.60	0%	47%	47%	7%	0	-3	+3	0	+0.10	0%	-10%	+10%	0%
R23	R59	Accuracy requirements for regular and stress cases	0	14	15	1	2.57	0%	47%	50%	3%	0	13	16	1	2.60	0%	43%	53%	3%	0	+1	-1	0	-0.03	0%	+3%	-3%	0%
P7	**P7**	**ACCURACY**	**0**	**10**	**20**	**0**	**2.67**	**0%**	**33%**	**67%**	**0%**	**0**	**9**	**21**	**0**	**2.70**	**0%**	**30%**	**70%**	**0%**	**0**	**+1**	**-1**	**0**	**-0.03**	**0%**	**+3%**	**-3%**	**0%**
R25	R62	Reporting in line with business model and risk profile	0	0	19	11	3.37	0%	0%	63%	37%	0	1	15	14	3.43	0%	3%	50%	47%	0	-1	+4	-3	-0.07	0%	-3%	+13%	-10%
P8	**P8**	**COMPREHENSIVENESS**	**0**	**1**	**20**	**9**	**3.27**	**0%**	**3%**	**67%**	**30%**	**0**	**2**	**20**	**8**	**3.20**	**0%**	**7%**	**67%**	**27%**	**0**	**-1**	**0**	**+1**	**+0.07**	**0%**	**-3%**	**0%**	**+3%**
R27	R74	Inventory and classification of risk data item	0	8	18	4	2.87	0%	27%	60%	13%	1	11	16	2	2.63	3%	37%	53%	7%	-1	-3	+2	+2	+0.23	-3%	-10%	+7%	+7%
P9	**P9**	**CLARITY AND USEFULNESS**	**0**	**1**	**25**	**4**	**3.10**	**0%**	**3%**	**83%**	**13%**	**0**	**1**	**26**	**3**	**3.07**	**0%**	**3%**	**87%**	**10%**	**0**	**0**	**-1**	**+1**	**+0.03**	**0%**	**0%**	**-3%**	**+3%**
R29	R81	Availability of all critical exposure reports shortly in stress situations	0	6	21	3	2.90	0%	20%	70%	10%	0	7	20	3	2.87	0%	23%	67%	10%	0	-1	+1	0	+0.03	0%	-3%	+3%	0%
P10	**P10**	**FREQUENCY**	**0**	**4**	**23**	**3**	**2.97**	**0%**	**13%**	**77%**	**10%**	**0**	**7**	**21**	**2**	**2.83**	**0%**	**23%**	**70%**	**7%**	**0**	**-3**	**+2**	**+1**	**+0.13**	**0%**	**-10%**	**+7%**	**+3%**
R31	R84	Timely dissemination of reports balanced with appropriate confidentiality	0	1	18	11	3.33	0%	3%	60%	37%	0	0	21	9	3.30	0%	0%	70%	30%	0	+1	-3	+2	+0.03	0%	+3%	-10%	+7%
P11	**P11**	**DISTRIBUTION**	**0**	**0**	**20**	**10**	**3.33**	**0%**	**0%**	**67%**	**33%**	**0**	**0**	**23**	**7**	**3.23**	**0%**	**0%**	**77%**	**23%**	**0**	**0**	**-3**	**+3**	**+0.10**	**0%**	**0%**	**-10%**	**+10%**

Annex 4: Additional questions related to large-scale IT/data related projects

Question 33. Please explain what strategic priority data/IT project has been given within the bank's portfolio of change projects. Please confirm that the entire project lifecycle (from initiation to implementation/delivery) has been funded by senior management.

Consistent throughout the G-SIB respondents, ongoing IT projects were described as "high priority" and "enterprise-wide". Most respondents identified multiple IT projects in place which were expected to achieve compliance with the Principles, reduce complexity, and improve efficiencies. Many G-SIBs prioritised projects by risk or market, given that multiple projects with competing resources were in progress. While not all firms commented on funding, those that did mentioned that IT projects were fully funded according to their normal budgeting/planning cycle. Only one respondent noted that no large scale information technology and data programs are needed to achieve full compliance with the Principles.

Question 34: Where the project/programme is not due to be complete by January 1 2016, please include in the comments an assessment if the project/programme can be rescheduled with higher priority without impacting other strategic priorities to fully comply with the Principles by the due date. If this is not possible, please discuss temporary measures will be put in place pending the completion of the project/programme to mitigate any material risks arising from gaps in compliance with the Principles.

Generally G-SIBs have commented that projects related to RDARR compliance have been given top priority, at the expense of other strategic priorities. Several commenters noted that resources are strained to meet changing regulatory initiatives. Other commenters admitted that given the scale and interdependencies of RDARR projects, altering delivery dates is difficult because that would negatively impact other initiatives and result in inadequate RDARR solutions. One commenter, expecting to have its integrated data infrastructure completed well past the January 2016 deadline, described the need to automate manual workarounds, establish the data management and governance policies to mitigate the risk associated with the delayed implementation.

Question 35: Please explain how senior management and control functions (eg operational risk and internal audit) maintain oversight of the progress of these projects/programmes.

Generally, the G-SIBs described longstanding processes to provide appropriate oversight for these projects. Self-assessments completed by first line business owners, controls for change management processes, and independent review by internal audit were identified as oversight mechanisms. Additionally, the existence of senior management oversight was mentioned to further support the notion that adequate oversight is in place for these critical projects. One G-SIB noted that "higher standards and oversight/transparency" are in place for large scale enterprise transformational programs.