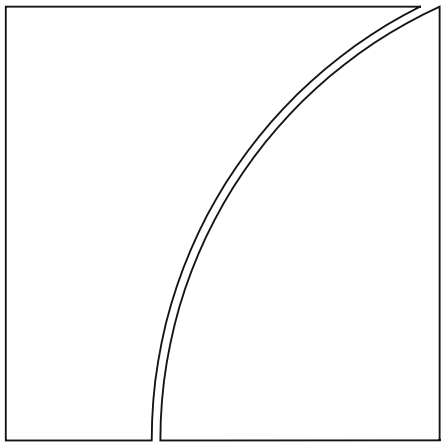
Basel Committee
on Banking Supervision



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

December 2015

BANK FOR INTERNATIONAL SETTLEMENTS

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

ISBN 978-92-9197-378-1 (print)

ISBN 978-92-9197-379-8 (online)

Contents

Principles for effective risk data aggregation and risk reporting: lessons learned for effective implementation

Introduction

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

One challenge in assessing banks' ability to comply with the framework stems from the fact that it is principles-based. That is, the Principles do not give objective or quantitative benchmarks, but, rather, indicate that banks' capabilities should be scaled to their business model and/or risk profile. This is true of any principles-based supervisory requirement, and was fully intended by the Committee. Therefore, it is important to understand the overall intent of the framework in addition to the specific requirements, the diversity of challenges different banks face and the range of supervisory approaches to promote compliance and remedy weaknesses.

The objective of this report is to draw out key lessons learned and elaborate key recommendations to further facilitate implementation. Overall, the Principles have been instrumental in motivating banks to improve their risk data aggregation and risk reporting capabilities. Noticeable gains have been made since the Principles were first published, particularly in establishing or strengthening internal governance frameworks, and, in general, increasing banks' awareness of the need to comply with these Principles to promote good risk management.

However, banks still fall short of full compliance, and additional work must be done to meet the intent of the Principles. As noted above, a tailored approach to assessment is warranted, but should be consistent with international standards. There remains an expectation that banks will continue to improve their internal frameworks and that supervisors will monitor progress and call on banks to redress observed weaknesses.

Section 1 (and Appendix 1) briefly reviews the objectives of the Principles, and Section 2 summarises the work conducted to date. Section 3 provides an overview of banks' progress towards compliance, including the main challenges faced. Section 4 highlights potential supervisory approaches to assessing compliance. Section 5 draws together insights into core lessons learned, while Section 6 provides key recommendations for the near to medium term.

1. Overall objectives of the Principles

The financial crisis that began in 2007 revealed that many banks, including global systemically important banks (G-SIBs), were unable to effectively aggregate risk exposures and identify concentrations fully, quickly and accurately. This seriously impaired the ability of banks to take adequate, effective and timely risk decisions, with wide-ranging consequences for the banks themselves and for financial system.

The Principles published in January 2013 are intended to:

- enhance the infrastructure for reporting key information, particularly for board and senior management;
- improve the decision-making process throughout the organisation by enhancing the management of information across legal entities and at the global consolidated level;

- reduce the probability and severity of losses resulting from risk management weaknesses;
- improve the speed at which information is available; and
- improve the organisation's quality of strategic planning and the ability to manage the risk of new products and services.

Effective and consistent implementation of the Principles underpins sound risk management practices and decision-making processes at banks, in turn improving the resilience of the overall banking system. Improving banks' ability to aggregate risk data will also improve their resolvability. Moreover, strong risk management capabilities will increase the value of a bank. Therefore, the long-term benefits will far outweigh the investment costs.

In order to achieve these benefits, the Principles provide guidance on the infrastructure and capacities that banks should have in place to improve risk management. This is important since non-compliance with international requirements that were created to remedy issues that arose during the financial crisis may hamper the ability of the sector as a whole to withstand future crises. The 11 Principles can be divided into three main pillars: (i) governance and infrastructure; (ii) data aggregation; and (iii) risk reporting (see Appendix 1).

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

2. Work conducted in 2011–15

Basel Committee work on risk data aggregation and risk reporting began in 2011, and, the Principles were published in January 2013. The deadline for implementation for banks identified as G-SIBs in November 2011 or November 2012[1] is 1 January 2016. Over 2013–15, the Committee published two reports on banks' self-assessment of their progress towards compliance with the Principles and conducted outreach with private sector stakeholders to better understand implementation challenges.

2.1 Bank self-assessment questionnaires (based on Principles 1–11)

In 2013 and 2014, banks completed two self-assessment questionnaires on their level of compliance with the requirements under Principles 1–11. Results of both self-assessments were published as progress reports, along with key recommendations to supervisors to facilitate banks' compliance with the Principles.

2.2 Surveys to supervisors (based on Principles 12–14)

Surveys were also conducted to assess supervisory progress in implementing Principles 12–14.

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

2.3 Exchange of information among supervisors on domestic developments

In 2015, work focused on exchange of information to gain a better understanding of the main weaknesses and challenges to timely and effective implementation of the Principles.

2.4 Outreach with industry

The Committee has conducted regular outreach with the banking industry, with the objective to understand the implementation challenges inherent in the Principles. This includes not only G-SIBs, but also other private sector stakeholders conducting similar analyses on banks' implementation practices. Given the persistent challenges with implementing the Principle on data architecture and IT infrastructure, the Committee also met with industry representatives and internal risk specialists.

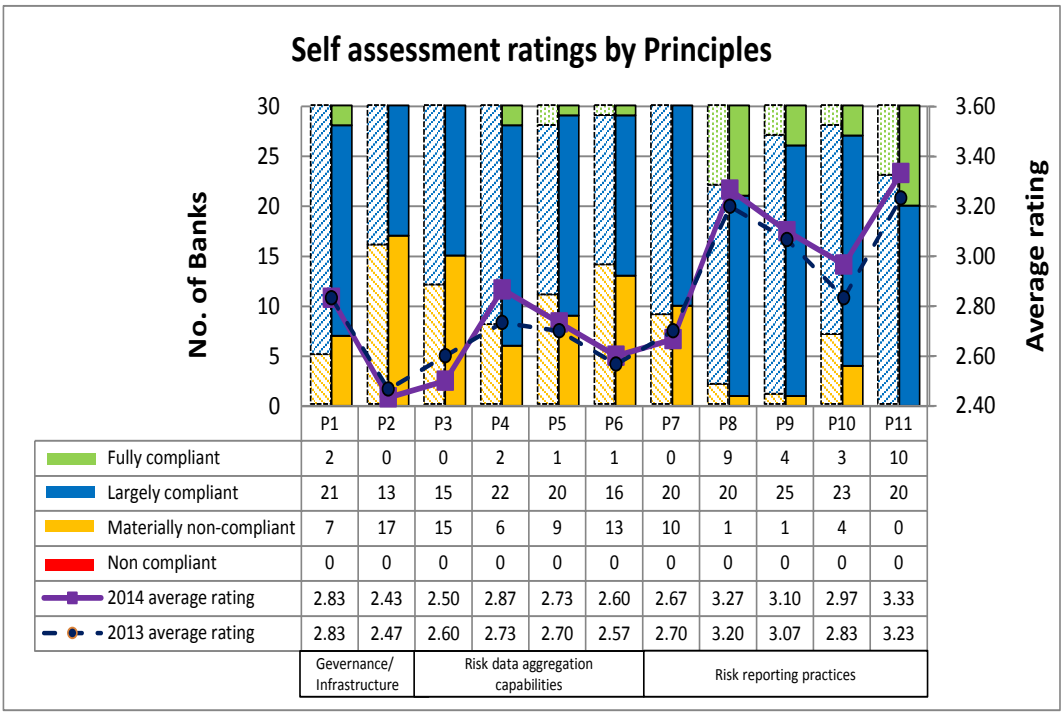
3. Banks' progress towards compliance: timelines and challenges

3.1 Banks' progress

Since the publication of the Principles, banks have made some progress towards compliance, particularly when compared with their pre-crisis status (based on past self-assessments). However, the 2014 progress report indicated, according to banks' self-assessments, that 14 G-SIBs will not fully comply with at least one of the 11 Principles by the deadline.[2] This compares to 10 banks in the 2013 progress report. Based on the 2014 progress report and supervisory monitoring, expected dates for full compliance with all Principles ranged from sometime in 2016 to as far out as 2018. As seen in Graph 1 below, in both 2014 and 2013, banks tended to assess their performance as best in risk reporting, with weaker self-assessed compliance in data aggregation, and governance and infrastructure. Those countries which have already designated domestic systemically important banks (D-SIBs) have made similar observations. Supervisors note that banks continue to make progress towards compliance, although with mixed results.

[2] Please note that a similar exercise was not conducted in 2015. Therefore, data shown in this section refers to the exercises reported on in 2014 and 2013. For more in-depth discussion of these survey results, please see Progress in adopting the principles for effective risk data aggregation and risk reporting (January 2015) and Progress in adopting the principles for effective risk data aggregation and risk reporting (December 2013).

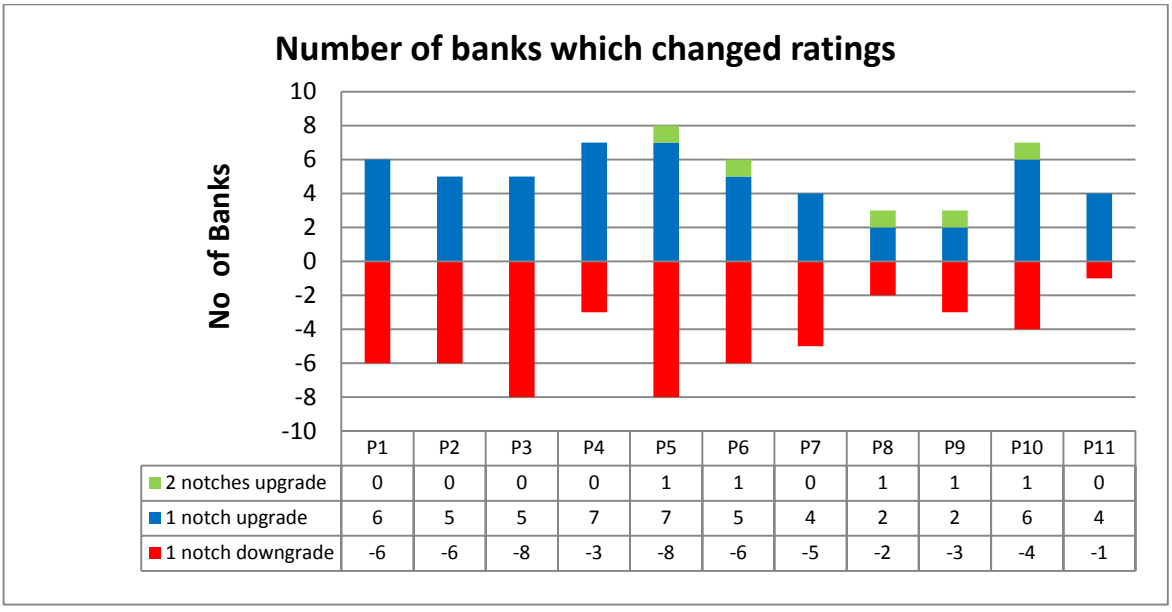
Graph 1



	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				

Moreover, as seen in Graph 2, banks' self-assessment ratings changed over time. The drivers vary; in some cases, improvements were driven by specific actions taken by banks (or completion of projects). In fact, in the 2014 progress report, there was evidence of a backward slide. This was due to a combination of factors, including an enhanced understanding of the requirements of the Principles or by practical exercises that objectively revealed deficiencies in banks' capabilities. More in-depth communication on supervisory expectations has helped further entrench understanding of the improvements needed.

Graph 2



	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

Nevertheless, banks acknowledge the importance of the Principles, and demonstrated that risk data aggregation should be a high priority.

3.2 Challenges to meeting the requirements of the Principles

Notwithstanding the encouraging developments noted above, the self-assessments, outreach with industry and supervisory oversight have shown that there remain some core challenges with achieving full compliance.

3.2.1 Defining key terminology

In terms of defining compliance, many of the requirements in the Principles focus on the concept of materiality, eg material business lines, entities and risks. Understandably, there is a desire for more uniform and objective thresholds. However, the Principles are clear that the concept of materiality is bank-specific and depends heavily on a bank's business model and risk exposures. For example, the ability to aggregate and assess market risk data may be less important for a largely retail bank. In another example, a supervisor may want a banking group with a number of large subsidiaries to also apply the Principles equally stringently at the solo level. In fact, as some subsidiaries of G-SIBs are D-SIBs in other jurisdictions, local entities may in fact be required to comply with the Principles on a standalone basis; this then requires strong coordination on the part of supervisors to establish expectations.

3.2.2 Data architecture and IT projects

Whether due to under-investment prior to the development of the Principles, or the significant costs associated with it, completing large-scale infrastructure projects on time continues to be seen as the most significant obstacle to full compliance. However, it should be noted that gains in infrastructure would enable banks not only to comply with Principle 2, but also to enhance their abilities to satisfy other Principles which rely heavily on sound and stable IT architecture, eg data aggregation.

Principle 2 had the lowest average rating in both 2013 and 2014, signalling that this was a critical area in need of improvement. Given the complexity of large-scale, ongoing, multi-year IT infrastructure projects and other data-related projects, there is still considerable work ahead. In 2014, one third of G-SIBs did not expect to adhere to Principle 2 by the deadline. While the other two thirds noted that they would be compliant by January 2016, there remains heightened execution risk of not meeting deadlines. Moreover, it was unclear whether banks had robust contingency plans in place to mitigate risks arising from delayed implementation of these long-term strategic projects.

3.2.3 Accuracy and adaptability of risk data

Significant gaps in terms of data accuracy and adaptability were also identified. Principle 3 (accuracy/integrity) and Principle 6 (risk data aggregation adaptability) had some of the lowest reported compliance ratings. In the 2014 self-assessments, eight G-SIBs noted that they would not be compliant at the implementation deadline, twice the number of banks that indicated this in 2013. Moreover, in 2014, half the banks rated themselves as materially non-compliant. This is most notable in the areas of unifying and rationalising the dictionaries and taxonomies of risk data repositories as well as establishing clear risk data ownership and responsibilities over the attendant quality controls. Increasing compliance levels in this area would require advances in three key areas.

First, the Principles note that there should be an appropriate balance between automated and manual systems. Despite this, concern remains about the use of manual processes, and how human error could lead to less accurate and/or less timely data. Supervisors judge a higher degree of automation as essential to reach the objective of the Principles. Overreliance on manual processes challenges banks' ability to aggregate risk data in a timely and accurate manner, particularly during stress/crisis situations. Reports indicate that high-frequency data, such as market and liquidity risk data, tend to be largely

automated, but manual processes are prevalent in other areas. Importantly, the ability to provide accurate data on a timely basis, eg during stress situations, is still very weak.

Second, there are also challenges associated with documentation of processes, particularly in large banking groups which operate in a number of jurisdictions or across a number of business lines. These differences impede the ability to formulate a common language, and develop "data dictionaries" to align definitions across different frameworks, as well as to align finance and risk terminology. This is further complicated by differences in accounting regimes across jurisdictions.

Third and related to both of these, the ability to adapt data processes, particularly for ad hoc requests, is persistently weak. In addition to banks' self-assessed low levels of compliance, evidence from practical applications shows that banks still struggle with delivering quality data decomposed and presented in different ways, particularly in a timely manner.

3.2.4 Risk reporting

As seen in Graph 1, banks consistently rated themselves highly on risk reporting practices. It is true that Principle 7 simply states that risk management reports should convey aggregated data in an exact manner. However, weaknesses in areas of data accuracy then mean that risk reports themselves will be inaccurate. The Committee has continually stressed this type of interdependency between the Principles, but it is still unclear whether this has been fully internalised by banks.

4. Supervisory approaches to assessing compliance: Principles 12–14

4.1 Supervisory review of compliance

As noted in Principle 12, supervisors should review and evaluate banks' compliance. Supervisors have indicated that there are several different approaches to fulfil their obligations in this regard. This includes bank-specific monitoring and specialised examinations on risk data aggregation and risk reporting capabilities. Supervisors indicated the use of thematic or horizontal reviews to supplement the assessment of banks' abilities to meet the Principles. In some cases, assessment of banks' risk data aggregation and reporting capabilities are, or could also be, incorporated into other supervisory practices, since accurate risk data are at the heart of risk management. Finally, the role of internal and external audit has taken on new prominence with regard to the need to certify or validate banks' compliance.

4.2 Supervisors' toolkit to address non-compliance

Principle 13 requires supervisors to use appropriate tools and resources to require effective and timely remedial action by a bank to address deficiencies in its risk data aggregation capabilities and risk reporting. Discussions with supervisors have indicated that they have several key tools at their disposal, either to promote compliance or to remedy shortcomings. In general, supervisors have a framework to escalate actions as weaknesses persist or intensify, in line with broader supervisory actions. Where specific regional arrangements exist, country-specific actions can be strengthened by a macro-oriented overlay. Specific tools are similar to those used to remedy non-compliance with other regulatory and supervisory requirements, ranging from the requirement to submit a remedial plan to being a contributing factor in additional capital charges.

4.4 Home-host cooperation

Principle 14 states that supervisors should cooperate with relevant supervisors in other jurisdictions regarding the supervision and review of the Principles, and the implementation of any remedial action if necessary. However, banks and authorities may be operating on different timelines or assessment frameworks.

The supervisors noted that it is highly likely that the usual home-host supervisory protocols will be followed to address any compliance issues, and this is probably especially true for jurisdictions with large foreign subsidiaries.

5. Key insights/lessons learned

5.1 Understanding and awareness of the framework

As noted previously, it is clear that banks generally no longer view adhering to the Principles as a simple compliance exercise. Most banks' managements understand the need for a transformation and have initiated projects, or at least aligned existing projects, to comply with the Principles. Industry outreach has indicated that banks are dedicating significant resources to completing projects.

Senior management and boards have slowly become more involved in improving architecture and processes, particularly as the 2016 deadline nears and supervisory oversight heightens. The higher budgetary requirements and the establishment of more senior positions have helped further facilitate a greater level of responsibility and board scrutiny.

While banks have begun to exhibit a better understanding of the overall objectives and goals on the framework, it is not clear that their understanding is sufficiently complete. For example, past self-assessments showed that banks did not appreciate the interdependencies between the Principles, eg that high-quality risk reporting relies on high-quality data aggregation.

In addition, supervisors' understanding of the framework is consistently improving. Awareness of the framework is increasingly being disseminated throughout and across supervisory authorities, and authorities are developing cross-departmental teams or fora. Supervisors are gathering information from a broad array of exercises, eg stress-testing and ad hoc information requests, to inform assessments of the Principles.

5.2 Implementation by banks

5.2.1 Defining and assessing compliance

As noted, the principles-based nature of the framework could result in different interpretations of full compliance. This is true of any principles-based supervisory requirements and was fully intended. However, this makes defining compliance challenging. On the one hand, compliance should be viewed as an offshoot of the objectives of the Principles.

Effective implementation of the Principles goes beyond a checklist approach. It requires an understanding of the objectives behind the requirements. The overall objective is to enable a bank to manage risk data and reporting in a manner that best suits its business model and risk profile. As a result, there is no "one size fits all" approach. On the other hand, there is still a need for some consistency in application across banks and jurisdictions.

In particular, the concept of materiality is important. The question is, who defines this and how can it be objectively measured. Principle 1 clearly states that a bank's board and senior management

have the primary responsibility, and all implementation should flow from that overarching governance structure. However, as with most risk management, authorities will review how banks' views and governance align with supervisory expectations. In doing so, particularly for both banks' and supervisors' assessment of compliance, a mix of quantitative thresholds and qualitative judgment are needed.

5.2.2 Governance

The Committee agrees that governance is critical to successful implementation of the Principles. There have been some improvements in banks' governance structures and responsibilities. Some banks have developed senior-level positions, with greater authority (and sometimes independent budgets) to manage data processes. In most banks, the need to certify their stated compliance levels has created a new internal audit role or independent validation units, and the role of internal and external audit has taken on a new dimension.

5.2.3 IT infrastructure and data aggregation processes

As noted above, upgrading IT infrastructure is a key hurdle to complete and timely implementation. Transforming an existing IT landscape is a long-lasting process, particularly developing high-quality yet tractable frameworks. Outreach with industry and other reports indicate that extensive merger and acquisition activities have exacerbated this challenge as differing systems across entities are not appropriately integrated.

As noted above, supervisors have highlighted a high degree of execution risk. It is possible that, in some circumstances, tactical mitigants, ie short-term approaches, may be used to meet supervisory expectations of compliance over the near term, while longer-term projects are being pursued. However, neither long-term projects nor the use of short-term mitigants are excuses for non-compliance.

5.2.4 Risk reporting

As seen in the progress reports, banks rated themselves quite highly on their risk reporting capabilities, ie most banks thought they would be compliant by the implementation deadline. As noted above, there are significant interdependencies between the categories of Principles. It would be inconsistent for a bank to say that it does not have very accurate data aggregation practices but produces accurate risk reports. For example, there are a number of challenges with incomplete data dictionaries, which should in fact hamper banks' ability to produce accurate and consistent reports.

5.2.5 Overall adherence to the Principles

There is an expectation that banks should meet all risk data aggregation and risk reporting principles simultaneously. However, there are likely to be trade-offs in degrees of compliance with all of the Principles, particularly where banks are still making progress towards full compliance. For example, banks may have the ability to aggregate information across a broad spectrum of risk categories, but may not be able to do so in a timely manner. Conversely, they may be able to aggregate exposures in one class of risk within a short time period, but with less accurate data than if more time were available.

When judging overall compliance, comments from supervisors indicated that a bank's business model and risk profile are key factors to consider. Both international standards and industry have highlighted the importance of processes to explain how they mitigate these risks, and justify these trade-offs through qualitative and, where possible, quantitative measures, eg back-testing. It is important to emphasise quality over timeliness; that is, it is more important to ensure that banks develop high-quality infrastructure rather than resorting to "band-aid" solutions to meet the implementation deadline.

6. Recommendations

Building on the observations above, this section highlights key recommendations to banks and supervisors. Appendix 2 highlights the evolution of past recommendations published by the Committee. It clearly shows that there are roles and responsibilities for both banks and supervisors, and they should build on the progress to date to continually strengthen both bank and supervisory practices. *In addition to these past recommendations*, the Committee stresses the following additional points.

6.1 Banks and supervisors should continue to promote understanding of the Principles

As noted above, stakeholders have been effective at disseminating learning about the Principles through firms and authorities. However, continuous efforts are needed. Authorities that do not already do so can leverage efforts to discuss implementation with other supervisory and policy departments, as well as across jurisdictions, eg supervisory colleges and crisis management groups. At banks, effective implementation requires all business units to understand the implications of the Principles, including for forward-looking risk management and business expansion. Moreover, banks could also share approaches with peers to learn from each other's experiences.

6.2 Supervisors should conduct more in-depth/specialised examinations on data aggregation requirements to evaluate weaknesses

Some areas of weakness are less visible, particularly during general supervisory examinations. Therefore, supervisors should conduct more in-depth assessments, particularly in the areas of accuracy and completeness of risk data, to assess weaknesses.

6.3 Banks should clearly articulate risk data aggregation and risk reporting expectations, in line with their risk appetite in both normal and stress periods

The framework is clear that common and clearly stated supervisory expectations regarding risk data aggregation and risk reporting are necessary. This requires banks and supervisors to come to a common understanding of the key concepts in the framework. One of the more important aspects of the framework is the concept of materiality. Therefore, bank management should be able to determine their strategy for achieving full compliance in line with their risk management framework and actively discuss these with supervisors. Banks' board and senior management should set their tolerance levels based on business models and risk profiles. Similarly, the bank should also set compliance expectations with regard to risk data aggregation and risk reporting which should be discussed with supervisors. Banks should also take into account the potential future impact of failing to provide risk data information to senior management and the board in charge of making key decisions at their institutions. Supervisors expect banks to be able to explain omissions of information, keeping the concept of materiality in focus. Importantly, senior management and the board should be involved in this decision.

Given the framework's principles-based requirements, banks should discuss expectations with supervisors. It is particularly important for a bank to explain its interpretation of the Principles and the chosen definition of materiality and tolerance levels to supervisors.

Moreover, compliance should be seen as a dynamic process, in which further improvements are needed periodically. Even banks that are considered compliant should strive for continuous improvements, taking into account developments in the operating environment, as risk profiles, data and reporting needs, and available technology could affect supervisory expectations. It is useful for

institutions to freely and consistently communicate with relevant supervision staff regarding any changes in implementation and interpretation of the Principles, including materiality and tolerance levels.

6.4 Banks should have governance arrangements in place for manual processes

The Principles note that a higher degree of automation is desirable to reduce the risk of errors in the development of risk reports. However, achieving full automation is not possible. It is important that banks have the appropriate controls around any manual processes. As a first step, banks should develop an internal identification/inventory of manual processes and validation of these processes to ensure they are working as intended.

6.5 Bank should critically examine their data architecture and data adaptability capabilities

Given the observed weaknesses in complying with infrastructure requirements and banks' persistent inability to improve in this area, the complexity of some G-SIBs' IT architecture may have reached an unmanageable level. Banks should consider reducing the complexity of their systems to aggregate risks in the required manner. As noted below, the importance of controls to ensure accurate data aggregation and reporting cannot be overstated.

6.6 Banks' compliance with the Principles should be subject to an independent evaluation in early 2016

An in-depth evaluation of banks' compliance with the Principles should be carried out by an independent party in early 2016. This independent evaluation could be conducted by either external or internal auditors. In both cases, the evaluating team should develop a certification procedure based on high standards of validation. Identified deficiencies should be reported to the board so that remedial actions can be taken as necessary.

6.7 In cases of non-compliance at the implementation deadline, banks should provide a remedial plan that is agreeable to supervisors

Management at banks that have inappropriately implemented the Principles should provide a remediation plan that highlights a reasonable timeline for correcting the deficiencies and is agreeable to supervisors. In particular, deficiencies noted in examination reports or audit findings should be reported to the bank's board. As the severity of the banks' weaknesses increases, additional supervisory measures could be taken. This can include Pillar II capital measures or even scaling back certain operations that present significant safety and soundness risk which the bank is unable to effectively monitor and report.

Banks should have policies and processes in place regarding the application of any trade-offs, and be able to explain the impact of these trade-offs on their decision-making process. In these cases, a clear description of controls should be included. There should be no trade-offs that materially impact risk management decisions. Senior management and the board should be aware of these trade-offs and their implications for risk management.

Appendix 1: Summary of the Principles

The Principles cover four closely related sections:

- Overarching governance and infrastructure
- Risk data aggregation capabilities
- Risk reporting practices
- Supervisory review, tools and cooperation

I. Overarching governance and infrastructure

Principle 1

Governance – A bank's risk data aggregation capabilities and risk reporting practices should be subject to strong governance arrangements consistent with other Principles and guidance established by the Basel Committee.[3]

Principle 2

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

II. Risk data aggregation capabilities

Principle 3

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

Principle 4

Completeness – A bank should be able to capture and aggregate all material risk data across the banking group. Data should be available by business line, legal entity, asset type, industry, region and

[3] See eg Basel Committee on Banking Supervision, *Principles for enhancing corporate governance*, October 2010, and *Enhancements to the Basel II framework*, July 2009.

other groupings, as relevant for the risk in question, that permit identifying and reporting risk exposures, concentrations and emerging risks.

Principle 5

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

Principle 6

Adaptability – A bank should be able to generate aggregate risk data to meet a broad range of on-demand, ad hoc risk management reporting requests, including requests during stress/crisis situations, requests due to changing internal needs and requests to meet supervisory queries.

III. Risk reporting practices

Principle 7

Accuracy - Risk management reports should accurately and precisely convey aggregated risk data and reflect risk in an exact manner. Reports should be reconciled and validated.

Principle 8

Comprehensiveness - Risk management reports should cover all material risk areas within the organisation. The depth and scope of these reports should be consistent with the size and complexity of the bank's operations and risk profile, as well as the requirements of the recipients.

Principle 9

Clarity and usefulness - Risk management reports should communicate information in a clear and concise manner. Reports should be easy to understand yet comprehensive enough to facilitate informed decision-making. Reports should include an appropriate balance between risk data, analysis and interpretation, and qualitative explanations. Reports should include meaningful information tailored to the needs of the recipients.

Principle 10

Frequency - The board and senior management (or other recipients as appropriate) should set the frequency of risk management report production and distribution. Frequency requirements should reflect the needs of the recipients, the nature of the risk reported, and the speed at which the risk can change, as well as the importance of reports in contributing to sound risk management and effective and efficient decision-making across the bank. The frequency of reports should be increased during times of stress/crisis.

Principle 11

Distribution - Risk management reports should be distributed to the relevant parties and while ensuring confidentiality is maintained.

IV. Supervisory review, tools and cooperation

Principle 12

Review - Supervisors should periodically review and evaluate a bank's compliance with the eleven Principles above.

Principle 13

Remedial actions and supervisory measures - Supervisors should have and use the appropriate tools and resources to require effective and timely remedial action by a bank to address deficiencies in its risk data aggregation capabilities and risk reporting practices. Supervisors should have the ability to use a range of tools, including Pillar 2.

Principle 14

Home/host cooperation - Supervisors should cooperate with relevant supervisors in other jurisdictions regarding the supervision and review of the Principles, and the implementation of any remedial action if necessary.

Appendix 2: Evolution of key recommendations of the Basel Committee

Evolution of key recommendations of the Basel Committee — Table A.1

2013	2014	2015
Supervisory authorities should consider enhancing their efforts to fully integrate the Principles in a comprehensive way within their supervisory programmes.	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.	Banks and supervisors should continue to promote understanding of the Principles.
Supervisory authorities should consider enhancing their efforts to test banks' capabilities to aggregate and produce reports in stress/crisis situations, including resolution.	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.	Supervisors should conduct more in-depth/specialised examinations on data aggregation requirements to evaluate weaknesses.
Supervisory authorities should consider enhancing their efforts to conduct thematic reviews.	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.	Banks should clearly articulate risk data aggregation and risk reporting expectations, in line with their risk appetite in both normal and stress periods
Supervisory authorities should consider enhancing their efforts to develop concrete supervisory plans or other supervisory tools for 2014 and 2015.	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.	Banks should have governance arrangements in place for manual processes.

Evolution of key recommendations of the Basel Committee

Table A.1

2013	2014	2015
na	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 (c) Quality controls in place	Banks should critically examine their data architecture and data adaptability capabilities.
na	Supervisory authorities should continue to actively exchange information on how they intend to facilitate compliance, or remedy non-compliance.	Banks' compliance with the Principles should be subject to an independent evaluation in early 2016.
na	na	In cases of non-compliance at the implementation deadline, banks should provide a remedial plan that is agreeable to supervisors.