Basel Committee
on Banking Supervision

Consultative Document

Principles for effective risk data aggregation and risk reporting

Issued for comment by 28 September 2012

June 2012

BANK FOR INTERNATIONAL SETTLEMENTS

Copies of publications are available from:

Bank for International Settlements
Communications
CH-4002 Basel, Switzerland

E-mail: publications@bis.org

Fax: +41 61 280 9100 and +41 61 280 8100

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

ISBN print: 92-9197-138-3
ISBN web: 92-9131-138-3

Contents

Comments on this consultative document should be submitted by Friday 28 September 2012 by e-mail to baselcommittee@bis.org. Alternatively, comments may be sent by post to the Secretariat of the Basel Committee on Banking Supervision, Bank for International Settlements, CH-4002 Basel, Switzerland. All comments will be published on the Bank for International Settlements' website unless a comment contributor specifically requests confidential treatment.

Task Force on SIB Supervision of the Standards Implementation Group

Chair:

Fernando Vargas, Bank of Spain, Madrid

Australia	Ms Heidi Richards (APRA)
Canada	Mr James Dennison (OSFI)
China	Mr Xianqiu Zhang (CBRC)
France	Mr Hedi Jeddi (FPSA)
Germany	Ms Angela Hofmann (Bundesbank) Mr Stefan Iwankowski (BAFIN)
Hong Kong SAR	Mr Sunny Yung (HKMA)
Italy	Mr Angelo Carriero (BoI)
Japan	Mr Mitsutoshi Adachi (BoJ) Mr Takao Miyamoto (JFSA)
Mexico	Mr Efrain Solorio (CNBV)
Netherlands	Ms Inge Veldhuis (DNB)
Spain	Ms Cristina Iglesias-Sarria (BoS) Ms Cecilia Lozano (BoS)
United Kingdom	Ms Jill Elaine Savager(FSA) Mr Ian Tower (FSA)
United States	Mr Joel Anderson (OCC) Ms Stacy Coleman (FRBNY) Mr Kirk Odegard (FRB)
Financial Stability Board	Ms Grace Sone
Financial Stability Institute	Mr Amarendra Mohan
Secretariat	Mr Juan Carlos Crisanto Ms Ruth Doubleday

Principles for effective risk data aggregation and risk reporting

Where is the wisdom we have lost in knowledge?
Where is the knowledge we have lost in information?

T. S. Eliot. The Rock (1934)

Introduction

1. One of the most significant lessons learned from the global financial crisis that began in 2007 was that banks' information technology (IT) and data architectures were inadequate to support the broad management of financial risks. Many banks lacked the ability to aggregate risk exposures and concentrations quickly and accurately at the bank group level, across business lines and between legal entities. Some banks were unable to manage their risks properly because of weak risk data aggregation capabilities and risk reporting practices. This had severe consequences to the banks themselves and the stability of the financial system as a whole.

2. In response, the Basel Committee issued supplemental Pillar 2 (supervisory review process) guidance[1] to enhance banks' ability to identify and manage bank-wide risks. In particular, the Committee emphasised that a sound risk management system should have appropriate management information systems (MIS)[2] at the business and bank-wide level. The Basel Committee also included references to data aggregation as part of its guidance on Principles for enhancing corporate governance.[3]

3. Improving banks' ability to aggregate risk data will improve their resolvability. For global systemically important banks (G-SIBs) in particular, it is essential for resolution authorities to have access to aggregate risk data that complies with the FSB's Key Attributes of Effective Resolution Regimes for Financial Insitutions[4] as well as the principles set out below. For recovery, strong forward-looking data will help banks and supervisors anticipate problems ahead. It will also improve the prospects of finding alternative options to restore financial strength and viability when the firm comes under severe stress. For example, it could improve the prospects of finding a suitable merger partner.

4. Many in the banking industry[5] recognise the benefits of improving their risk data aggregation capabilities and are working towards this goal. They see the improvements in terms of strengthening the capability and the status of the risk function to make judgements. This leads to gains in efficiency, reduced probability of losses and enhanced strategic decision-making, and ultimately increased profitability. Supervisors observe that making improvements in risk data aggregation capabilities and risk reporting practices remains a challenge for banks, and supervisors would like to see more progress, in particular, at

---

1 *Enhancements to the Basel II framework* (July 2009) www.bis.org/publ/bcbs158.pdf.

2 MIS in this context refers to risk management information.

3 *Principles for enhancing corporate governance* (October 2010) www.bis.org/publ/bcbs176.pdf.

4 Key Attributes of Effective Resolution Regimes for Financial Institutions, Financial Stability Board, www.financialstabilityboard.org/publications/r_111104dd.pdf (October 2011).

5 See Institute of International Finance report, *Risk IT and Operations: Strengthening capabilities.* (June 2011).

G-SIBs. Moreover, as the memories of the crisis fade over time, there is a danger that the enhancement of banks' capabilities in these areas may receive a slower-track treatment. This is because IT systems, data and reporting processes require significant investments of financial and human resources with benefits that may only be realised over the long-term.

5. The Financial Stability Board (FSB) has several international initiatives underway to ensure continued progress is made in strengthening firms' risk data aggregation capabilities and risk reporting practices, which is essential to support financial stability. These include:

- The development of the *Principles for effective risk data aggregation and risk reporting* included in this report. This work stems from a recommendation in the FSB's *Progress report on implementing the recommendations on enhanced supervision,* issued on 4 November 2011:

  "The FSB, in collaboration with the standard setters, will develop a set of supervisory expectations to move firms', particularly SIFIs, data aggregation capabilities to a level where supervisors, firms, and other users (eg, resolution authorities) of the data are confident that the MIS reports accurately capture the risks. A timeline should be set for all SIFIs to meet supervisory expectations; the deadline for G-SIBs to meet these expectations should be the beginning of 2016, which is the date when the added loss absorbency requirement begins to be phased in for G-SIBs."

- The development of a new common data template for global systemically important financial institutions (G-SIFIs) in order to address key information gaps identified during the crisis, such as bi-lateral exposures and exposures to countries/sectors/instruments. This should provide the authorities with a stronger framework for assessing potential systemic risks.
- A public-private sector initiative to develop a Legal Entity Identifier (LEI) system. The LEI system will identify unique parties to financial transactions across the globe and is designed to be a key building block for improvements in the quality of financial data across the globe.

Definition

6. For the purpose of this paper and the principles, the term "risk data aggregation" means defining, gathering and processing risk data according to the bank's risk reporting requirements to enable the bank to measure its performance against its risk tolerance/appetite. This includes sorting, merging or breaking down sets of data.

Objectives

7. This paper presents a set of principles to strengthen banks' risk data aggregation capabilities and risk reporting practices. In turn this will enhance banks' risk management. National supervisors expect G-SIBs to implement these principles by 2016 and will assess their implementation starting in 2013 and share with the FSB from the end of 2013.

8. The adoption of these principles will enable fundamental improvements to the management of banks. These principles are expected to support a bank's efforts to:

- Enhance the infrastructure for reporting key information, particularly that used by the board and senior management to identify, monitor and manage risks;
- Improve the decision-making process throughout the banking organisation;
- Enhance the management of information across legal entities, while facilitating a comprehensive assessment of risk exposures 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 hence decisions can be made; and
- Improve the organisation's quality of strategic planning and the ability to manage the risk of new products and services.

9. Strong risk management capabilities are an integral part of the franchise value of a bank. Effective implementation of the principles should increase the value of the bank. The Committee believes that the long-term benefits of improved risk data aggregation capabilities and risk reporting practices will outweigh the initial investment costs incurred by banks.

10. For bank supervisors, these principles will complement other efforts to improve the intensity and effectiveness of G-SIB supervision. For resolution authorities, improved risk data aggregation should enable smoother G-SIB resolution, thereby reducing the potential recourse to taxpayers.

Scope and initial considerations

11. These principles are initially addressed to SIBs[6] and apply at both the banking group and on a solo basis. Common and clearly stated supervisory expectations regarding risk data aggregation and risk reporting are necessary for these institutions. National supervisors may nevertheless choose to apply the principles to a wider range of banks, in a way that is proportionate to the size, nature and complexity of these banks' operations.

12. The principles and supervisory expectations contained within this paper apply to a bank's risk management data. This includes data that is critical to enabling the bank to manage the risks it faces. Risk data and reports should provide management with the ability to monitor and track risks relative to the bank's risk tolerance/appetite.[7] The data should be forward-looking to provide early warnings of any potential breaches of risk limits that may be against the bank's risk appetite.

13. These principles also apply to all key internal risk management models, including but not limited to, Pillar 1 regulatory capital models (eg internal ratings-based approaches for credit risk and advanced measurement approaches for operational risk), Pillar 2 capital models and other key risk management models (eg value-at-risk).

---

[6] The expectations for G-SIBs and SIBs are the same, only the timeline is different.

[7] "Risk appetite is the level and type of risk a firm is able and willing to assume in its exposures and business activities, given its business objectives and obligations to stakeholders" as defined by the Senior Supervisors Group report, *Observations on Developments in Risk Appetite Frameworks and IT Infrastructure,* December 2010.

14. These principles apply to a bank's group risk management processes and supervisory reporting; however, banks may also benefit from applying the principles to other processes, such as financial and operational processes.

15. Finally, all the principles included in this paper are also applicable to processes that have been outsourced to third parties.

16. The principles cover four closely related topics:

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

17. Risk data aggregation capabilities and risk reporting practices are considered separately in this paper, but they are clearly inter-linked and cannot exist in isolation. High quality management reports rely on the existence of strong risk data aggregation capabilities, and sound infrastructure and governance ensures the information flow from one to the other. These risk data aggregation capabilities should meet all of the following principles simultaneously, ie there should be no trade-offs that materially inhibit risk management decisions.

18. National banking supervisors will start discussing implementation of the principles with senior management G-SIBs in early 2013. This will ensure that they develop a strategy to meet the principles by 2016.

19. The Basel Committee will track G-SIBs progress towards complying with the principles through its Standards Implementation Group (SIG) from 2013. This will include any observations on the effectiveness of the principles themselves and whether any enhancements or other revisions of the principles are necessary in order to achieve the desired outcomes. The Basel Committee will share its findings with the FSB at least annually.

I. Overarching governance and infrastructure

20. A bank should have in place a strong governance framework, risk data architecture and IT infrastructure. These are pre-conditions to ensure compliance with the other principles included in this document. In particular, a bank's board and senior management should take ownership of implementing all the risk data aggregation and risk reporting principles and have a strategy to meet them within a timeframe agreed with their supervisors. For a G-SIB this means by 2016 at the latest.

Principle 1

Governance – A bank's risk data aggregation capabilities and risk reporting practices should be subject to strong governance consistent with other principles and guidance established by the Basel Committee.[8]

21. A bank's board and senior management should promote the identification, assessment and management of data quality risks as part of its overall risk management framework. The framework should include agreed service level standards for both outsourced and in-house risk data-related processes, and a firm's policies on data confidentiality, integrity and availability, as well as risk management policies. A bank's board and senior management should review and approve the bank's group risk data aggregation and risk reporting and ensure that adequate resources are deployed.

22. A bank's risk data aggregation capabilities and risk reporting practices should be:

(a) Fully documented and subject to high standards of validation. This validation should be independent and include review of compliance with the principles in this document. The validation should review the appropriateness and effectiveness of the bank's risk data aggregation capabilities and risk reporting practices, and the quality of the governance surrounding the processes. Independent validation could mean a review by the internal audit function. However, best practice would suggest that an independent validation unit with specific IT, data and reporting knowledge may be better positioned to perform this review. When such an independent validation unit exists, the internal audit function would still review its validation work as part of the audit plan.

(b) Considered as part of any new initiatives, including acquisitions and/or divestitures, new product development, as well as broader process and IT change initiatives. When considering a material acquisition, a bank's due diligence process should assess the risk data aggregation capabilities and risk reporting practices of the acquired entity, as well as the impact on its own risk data aggregation capabilities and risk reporting practices. The impact on risk data aggregation should be considered explicitly by the board and inform the decision to proceed. The bank should establish a timeframe to integrate and align the acquired risk data aggregation capabilities and risk reporting practices within its own framework.

(c) Unaffected by the bank's group structure. The group structure should not hinder risk data aggregation capabilities at a consolidated level or at any relevant level within the organisation (eg sub-consolidated level, jurisdiction of operation level). In

[8] *Principles for Enhancing Corporate Governance,* Basel Committee on Banking Supervision, October 2010; *Enhancements to the Basel II framework,* Basel Committee on Banking Supervision, July 2009.

particular, risk data aggregation capabilities should be independent from the choices a bank makes regarding its legal organisation and geographical presence.[9]

23. A bank's board and senior management should be fully aware of any limitations that prevent full risk data aggregation, in terms of coverage (eg risks not captured or subsidiaries not included), in technical terms (eg model performance indicators or degree of reliance on manual processes) or in legal terms (legal impediments to data sharing across jurisdictions). A bank's IT strategy should include improving risk data aggregation capabilities and risk reporting practices to remedy any shortcomings against the principles set forth in this report, and to match the evolving needs of the business. A bank should identify data critical to risk data aggregation and IT infrastructure initiatives through its strategic IT planning process, and support these initiatives through the allocation of appropriate levels of financial and human resources.

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.

24. Risk data aggregation capabilities and risk reporting practices should be given direct consideration as part of a bank's business continuity planning processes and be subject to a business impact analysis.

25. A bank should establish integrated[10] data taxonomies and architecture across the banking group, which includes information on the characteristics of the data (metadata), as well as use of single identifiers and/or unified naming conventions for data including legal entities, counterparties, customers and accounts.

26. Roles and responsibilities should be established as they relate to the ownership and quality of risk data and information for both the business and IT functions. The owners (business and IT functions), in partnership with risk managers, should ensure there are adequate controls throughout the lifecycle of the data and for all aspects of the technology infrastructure. The role of the business owner includes ensuring data is correctly entered by the relevant front office unit, kept current and aligned with the data definitions, and also ensuring that risk data aggregation capabilities and risk reporting practices are consistent with firms' policies.

II. Risk data aggregation capabilities

27. Banks should develop and maintain strong risk data aggregation capabilities to ensure that risk management reports reflect the risks accurately (ie meeting data aggregation expectations is necessary to meet reporting expectations). Compliance with these principles should not be at the expense of each other. These risk data aggregation capabilities should

[9] While taking into account any legal impediments to sharing data across jurisdictions.

[10] G-SIBs do not necessarily need to have one data model; rather, there should be robust automated reconciliation procedures where multiple models are in use.

meet all of the following principles below simultaneously (ie no trade-offs that materially inhibit risk management decisions).

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.

28. A bank should aggregate risk data in a way that is accurate and reliable.

(a) Controls surrounding risk data should be as robust as those applicable to accounting data.

(b) Where a bank relies on manual processes and desktop applications (eg spreadsheets, databases) and has specific risk units that use these applications for software development, it should have effective mitigants in place (eg end-user computing policies and procedures) and other effective controls that are consistently applied across the bank's processes.

(c) Risk data should be reconciled to accounting data, as well as to a bank's sources and books of record, to ensure that the risk data is accurate.

(d) A bank should strive towards a single authoritative source for risk data.

(e) A bank's risk personnel should have sufficient access to risk data to ensure they can appropriately aggregate, validate and reconcile the data to risk reports.

29. As a precondition, a bank should have a "dictionary" of the concepts used, such that data is defined consistently across an organisation.

30. There should be an appropriate balance between automated and manual systems. Where professional judgements are required, human intervention may be appropriate. For many other processes, a higher degree of automation is desirable to reduce the risk of errors.

31. Supervisors expect banks to document and explain all of their risk data aggregation processes whether automated or manual (judgement based or otherwise). Documentation should include an explanation of the appropriateness of any manual workarounds, a description of their criticality to the accuracy of risk data aggregation and proposed actions to reduce the impact.

32. Supervisors expect banks to develop metrics to monitor the accuracy of data and for appropriate escalation channels and action plans to be in place to rectify poor data quality. Supervisors could expect banks to monitor and report on the number of data items that are received, compared to the number of items expected.

Principle 4

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

33. A bank's risk data aggregation capabilities should include all material risk exposures, including those that are off-balance sheet.

34. A banking organisation is not required to express all forms of risk in a common metric or basis, but risk data aggregation capabilities should be the same regardless of the choice of risk aggregation systems implemented. However, each system should make clear the specific approach used to aggregate exposures for any given risk measure, in order to allow the board and senior management to assess the results properly.

35. Supervisors expect banks to produce aggregated risk data that is complete and to develop metrics to measure the completeness of their risk data. Where risk data is not entirely complete, the impact should not be critical to the bank's ability to manage its risks effectively. Supervisors expect banks to affirm that their data is materially complete, with any exceptions identified and explained.

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. This timeliness should meet bank-established frequency requirements for normal and stress/crisis risk management reporting.

36. A bank's risk data aggregation capabilities should ensure that it is able to produce aggregate risk information on a timely basis (in respect of a reference date) to meet all risk management reporting requirements.

37. The Basel Committee acknowledges that different types of data will be required at different speeds, depending on the type of risk, and that certain risk data may be needed faster in a crisis situation. Banks need to build their risk systems to be capable of producing aggregated risk data rapidly during times of crisis for all critical risks.

38. Critical risks include but are not limited to:

(a) The aggregated credit exposure to a large corporate borrower on the supervisory watchlist. By comparison, groups of retail exposures may not change as critically in a short period of time but may still include significant concentrations;

(b) Counterparty credit risk exposures, including, for example, derivatives;

(c) Trading exposures, positions, operating limits, and market concentrations by sector and region data;

(d) Liquidity risk indicators such as cash flows/settlements and funding; and

(e) Operational risk indicators that are time-critical (eg systems availability, unauthorised access).

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 crisis situations, requests due to changing internal needs and requests to meet supervisory queries.

39. A bank's risk data aggregation capabilities should be flexible and adaptable to meet ad hoc data requests as needed, and forward-looking to assess emerging risks. Adaptability will enable banks to conduct better risk management, including forecasting information, as well as to support stress testing and scenario analyses.

40. Adaptability includes:

(a) Data aggregation processes that are flexible and enable risk data to be aggregated for assessment and quick decision-making;

(b) Capabilities for data customisation to users' needs (eg dashboards, key takeaways, anomalies), to drill down as needed, and to produce "flash" summary reports;

(c) Capabilities to incorporate new developments on the organisation of the business and/or external factors that influence the bank's risk profile or the requirements to measure its components; and

(d) Capabilities to incorporate changes in the regulatory framework.

41. Supervisors expect banks to be able to generate subsets of data based on requested scenarios or resulting from economic events. For example, a bank should be able to aggregate risk data quickly on country credit exposures[11] as of a specified date based on a list of countries, as well as industry credit exposures as of a specified date based on a list of industry types across all business lines and geographic areas.

III. Risk reporting practices

42. Accurate, complete and timely data is a foundation for effective risk management. However, data alone does not guarantee that the board and senior management will receive appropriate information to make effective decisions about risk. To manage risk effectively, the right information needs to be presented to the right people at the right time. Risk reports based on risk data should be accurate, clear and complete. They should contain the correct content and be presented to the appropriate decision-makers in a time that allows for an appropriate response. A bank's risk management reports should contribute to sound risk management and decision-making by their relevant recipients, including, in particular, the board and senior management. To ensure the usefulness of these reports, they should comply with the following principles. Compliance with these principles should not be at the expense of each other.

[11] Including sovereign, bank, corporate and retail exposures, for example.

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.

43. Risk management reports should be accurate and precise to ensure a bank's board and senior management can rely with confidence on the aggregated information to make critical decisions about risk.

44. To ensure the accuracy of the reports, a bank should maintain, at a minimum, the following:

(a) Defined requirements and processes to reconcile reports to risk data;

(b) Automated and manual edit and reasonableness checks, including an inventory of the validation rules that are applied to quantitative information. The inventory should include explanations of the conventions used to describe any mathematical or logical relationships that should be verified through these validations or checks; and

(c) Integrated procedures for identifying, reporting and explaining data errors or weaknesses in data integrity via exceptions reports.

45. Supervisors expect that a bank's board and senior management should establish accuracy and precision requirements for both regular and crisis reporting, including critical position and exposure information. These requirements should reflect the criticality of decisions that will be based on this information.

46. Supervisors expect banks to consider accuracy requirements analogous to accounting materiality. For example, if omission or misstatement could influence the risk decisions of users, this may be considered material. A bank should be able to support the rationale for accuracy requirements. Supervisors expect a bank to consider precision requirements based on validation, testing or reconciliation processes and results.

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.

47. Risk management reports should include exposure and position information for all significant risk areas (eg credit risk, market risk, liquidity risk, operational risk) and all significant components of those risk areas (eg single name, country and industry sector for credit risk). Risk management reports should also cover risk-related measures (eg regulatory and economic capital).

48. Reports should identify emerging risk concentrations and provide information in the context of limits and risk appetite/tolerance and proposed recommendations for action where appropriate. Risk reports should include the current status of measures agreed by the board or senior management to reduce risk or deal with specific risk situations. This includes providing the ability to monitor emerging trends through forward-looking forecasts and stress tests.

49. Supervisors expect that risk management reports will be complete. A bank should determine risk reporting requirements to best suit its own business models and risk profiles. Supervisors will need to be satisfied with the choices a bank makes in terms of risk coverage, analysis and interpretation, scalability and comparability across group institutions. For example, an aggregated risk report should include, but not be limited to, the following information: capital adequacy, regulatory capital, capital and liquidity ratio projections, credit risk, market risk, operational risk, liquidity risk, stress testing results, inter- and intra-risk concentrations, and funding positions and plans.

50. Supervisors expect that risk management reports to the board and senior management provide a forward-looking assessment of risk and should not just rely on current and past data. The reports should contain forecasts or scenarios for key market variables and the effects on the bank so as to inform the board and senior management of the likely trajectory of the bank's capital and risk profile in the future.

Principle 9

Clarity - 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.

51. A bank's risk reports should contribute to sound risk management and decision-making by their relevant recipients, including, in particular, the board and senior management. Risk reports should ensure that information is meaningful and tailored to the needs of the recipients.

52. The balance of qualitative versus quantitative information will vary at different levels within the organisation and will also depend on the level of aggregation that is applied to the reports. Higher up in the organisation, more aggregation is expected and therefore a greater degree of qualitative interpretation will be necessary.

53. As one of the key recipients of risk management reports, the bank's board is responsible for determining its own risk reporting requirements and complying with its obligations to shareholders and other relevant stakeholders. The board should ensure that it is asking for and receiving relevant information that will allow it to fulfill its governance mandate relating to the bank and the risks to which it is exposed. This will allow the board to ensure it is operating within its risk-bearing capacity.

54. The board should also provide feedback to senior management when the risk reports do not meet its requirements and do not provide the right level and type of information to set and monitor adherence to the bank's risk appetite. The board should indicate whether it is receiving the right balance of detail and quantitative versus qualitative information.

55. Senior management is one of the key recipients of risk reports and is also responsible for determining its own risk reporting requirements. Senior management should ensure that it is receiving relevant information that will allow it to fulfill its management mandate relative to the bank and the risks to which it is exposed.

56. A bank should develop an inventory and classification of risk data items which includes a reference to the concepts used to elaborate the reports.

57. Supervisors expect that reports will be clear and useful. Reports should reflect an appropriate balance between detailed data, qualitative discussion, explanation and recommended conclusions. Interpretation and explanations of the data, including observed trends, should be clear.

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/efficient decision-making across the bank. The frequency of reports should be increased during times of crisis.

58. The frequency of risk reports will vary according to the type of risk, purpose and recipients. A bank should assess periodically the purpose of each report and set requirements for how quickly the reports need to be produced in both normal and crises situations. A bank should routinely test its ability to produce accurate reports within established timeframes, particularly in crisis situations.

59. Supervisors expect that in times of crisis all relevant and critical credit, market and liquidity position/exposure reports are available within a very short period of time to react effectively to evolving risks. Some position/exposure information may be needed immediately (intraday) to allow for timely and effective reactions.

Principle 11

Distribution - Risk management reports should be distributed to the relevant parties and include meaningful information tailored to the needs of the recipients, while ensuring confidentiality is maintained.

60. Reporting policies and procedures should recognise the differing information needs of the board, senior management, and the other levels of the organisation (for example risk committees). Procedures should be in place to allow for rapid collection and analysis of risk data and dissemination of reports to provide for timely presentation to all appropriate recipients. This should be balanced with the need to ensure confidentiality as appropriate.

61. Supervisors expect a bank to confirm periodically with recipients that the amount of information aggregated and produced in reports is relevant and appropriate to the governance and decision-making process, in line with Principle 9 on clarity.

IV. Supervisory review, tools and cooperation

62. Supervisors will have an important role to play in monitoring and providing incentives for a bank's implementation of, and ongoing compliance with the principles. They should also review compliance with the principles across banks to determine whether the principles themselves are achieving their desired outcome and whether further enhancements are required.

Principle 12

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

63. Supervisors should review a bank's compliance with the principles in the preceding sections. Reviews should be incorporated into the regular programme of supervisory reviews and may be supplemented by thematic reviews covering multiple banks with respect to a single or selected issue. Supervisors may test a bank's compliance with the principles through occasional requests for information to be provided on selected risk issues (for example, exposures to certain risk factors) within short deadlines, thereby testing the capacity of a bank to aggregate risk data rapidly and produce risk reports. Supervisors should have access to the appropriate reports to be able to perform this review.

64. Supervisors should draw on reviews conducted by the internal and external auditors to inform their assessments of compliance with the principles. Supervisors may require work to be carried out by a bank's internal audit functions or by experts independent from the bank. Supervisors must have access to all appropriate documents such as internal validation and audit reports, and should be able to meet with and discuss risk data aggregation capabilities with the external auditors when appropriate.

65. Supervisors should test a bank's capabilities to aggregate data and produce reports in both crisis and steady-state environments, including sudden sharp increases in business volumes.

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.

66. Supervisors should require effective and timely remedial action by a bank to address material deficiencies in its risk data aggregation capabilities and risk reporting practices and internal controls.

67. Supervisors should have a range of tools at their disposal to address material deficiencies in a bank's risk data aggregation capabilities. Such tools may include, but are not limited to, requiring a bank to take remedial action; increasing the intensity of supervision; requiring an independent review by a third party, such as external auditors; and the possible use of capital add-ons as both a risk mitigant and incentive under Pillar 2.[12]

68. Supervisors should be able to set limits on a bank's risks or the growth in their activities where deficiencies in data aggregation are assessed as causing significant weaknesses in risk management capabilities.

69. For new business initiatives, supervisors may require that robust risk data aggregation capabilities are demonstrated before allowing a new business venture or acquisition to proceed.

---

[12] *Enhancements to the Basel II framework* (July 2009) – Supplemental Pillar 2 guidance.

70. When a supervisor requires a bank to take remedial action, the supervisor should set a timetable for completion of the action. Supervisors should have escalation procedures in place to require more stringent or accelerated remedial action in the event that a bank does not adequately address the deficiencies identified, or in the case that supervisors deem further action is warranted.

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.

71. Effective cooperation and appropriate information sharing between the home and host supervisory authorities should contribute to the robustness of a bank's risk management practices across a bank's operations in multiple jurisdictions.

72. Cooperation can take the form of sharing of information within the constraints of applicable laws, as well as discussion between supervisors on a bilateral or multilateral basis (eg through colleges of supervisors), including, but not limited to, regular meetings. Communication by conference call and email may be particularly useful in tracking required remedial actions. Cooperation through colleges should be in line with the Basel Committee's *Good practice principles on supervisory colleges*.[13]

73. Supervisors should discuss their experiences regarding the quality of risk data aggregation capabilities and risk reporting practices in different parts of the group. This should include any impediments to risk data aggregation and risk reporting arising from cross-border issues and also whether risk data is distributed appropriately across the group. Such exchanges will enable supervisors to identify significant concerns at an early stage and to respond promptly and effectively.

V. Timelines / transitional arrangements

74. Supervisors expect that a bank's data and IT infrastructures will be enhanced in the coming years to ensure that its risk data aggregation capabilities and risk reporting practices are sufficiently robust and flexible enough to address their potential needs in normal times and particularly during times of crisis.

75. In order for G-SIBs to meet the principles in accordance with the 2016 timeline, national banking supervisors will discuss banks' analysis of risk data aggregation capabilities with their senior management and agree to timelines for required improvements. Supervisory approaches are likely to include requiring self-assessments by G-SIBs against these expectations in early 2013, with the goal of closing significant gaps before 2016. Supervisors may also engage technical experts to support their assessments of banks' plans in respect of the 2016 deadline.

[13] *Good practice principles on supervisory colleges* (October 2010) www.bis.org/publ/bcbs177.pdf

Annex 1

Accuracy	Closeness of agreement between a measured quantity value and a true quantity value.
Adaptability	The ability to change (or be changed) to respond efficiently and promptly to particular circumstances.
Clarity	Easy to understand and free from indistictness or ambiguity.
Completeness	Containing all relevant information over the relevant time horizon.
Comprehensiveness	Including or dealing with all aspects of something.
Distribution	The people or groups that receive the risk reports.
Frequency	The period of time between risk reports being generated.
Integrity	Data that has not been altered in an unauthorised manner and that is free from unauthorised manipulation that compromises accuracy, completeness or reliability.
Manual workarounds	Employing human-based processes and tools to tranfer, manipulate or alter data.
Precision	Degree to which repeated measurements under unchanged conditions show the same results.
Reconciliation	Aprocess used to compare two sets of data to ensure the figures are in agreement.
Risk appetite	The level and type of risk a firm is able and willing to assume in its exposures and business activities, given its business and obligations to stakeholders. It is generally expressed through both quantitative and qualitative means.
Risk Data aggregation	Defining, gathering, and processing risk data according to the bank's risk reporting requirements to enable the bank to measure its performance against its risk tolerance/appetite. This includes sorting, merging or breaking down sets of data.
Timeliness	Ability to provide risk data at a predefined point in time.
Validation	The process of ensuring the correctness of inputs, processing, and outputs prior to, during, and subsequent to, risk data aggregation and risk reporting.

Annex 2

Summary of the principles

The principles cover four closely related sections:

(i) Overarching governance and infrastructure

(ii) Risk data aggregation capabilities

(iii) Risk reporting practices

(iv) 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 consistent with other principles and guidance established by the Basel Committee.[14]

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,

[14] See *Principles for Enhancing Corporate Governance,* Basel Committee on Banking Supervision*,* October 2010; *Enhancements to the Basel II framework*, Basel Committee on Banking Supervision, July 2009.

industry, region and other groupings that permit identifying and reporting risk exposures, concentrations and emerging risks.

Principle 5

Timeliness – A bank should be able to generate aggregate and updated 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. This timeliness should meet bank-established frequency requirements for normal and stress/crisis risk management reporting.

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 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 - 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.

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/efficient decision-making across the bank. The frequency of reports should be increased during times of crisis.

Principle 11

Distribution - Risk management reports should be distributed to the relevant parties and include meaningful information tailored to the needs of the recipients, 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.