Basel Committee on Banking Supervision

SRP

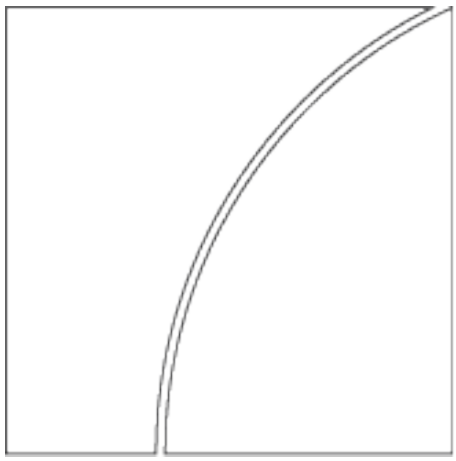
Supervisory review process

SRP36

Risk data aggregation and risk reporting

Version effective as of 15 Dec 2019

First version in the format of the consolidated framework.



BANK FOR INTERNATIONAL SETTLEMENTS

Objectives

36.1 This chapter presents a set of principles to strengthen banks' risk data aggregation capabilities and internal risk reporting practices (the Principles). The Principles are expected to support a bank's efforts to:

(1) enhance the infrastructure for reporting key information, particularly that used by the board and senior management to identify, monitor and manage risks;

(2) improve the decision-making process throughout the banking organisation;

(3) enhance the management of information across legal entities, while facilitating a comprehensive assessment of risk exposures at the global consolidated level;

(4) reduce the probability and severity of losses resulting from risk management weaknesses;

(5) improve the speed at which information is available and hence decisions can be made; and

(6) improve the organisation's quality of strategic planning and the ability to manage the risk of new products and services.

36.2 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 investment costs incurred by banks.

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

Scope and general provisions

36.4 These Principles apply to systemically important banks (SIBs) and apply at both the banking group and on a solo basis.

36.5 The Principles and supervisory expectations contained in SRP36 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.

36.6 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).

36.7 The Principles apply to a bank's group risk management processes. However, banks may also benefit from applying the Principles to other processes, such as financial and operational processes, as well as supervisory reporting.

36.8 All the Principles are also applicable to processes that have been outsourced to third parties.

36.9 The Principles cover four closely related topics:

(1) Overarching governance and infrastructure (Principles 1 and 2)

(2) Risk data aggregation capabilities (Principles 3, 4, 5 and 6)

(3) Risk reporting practices (Principles 7, 8, 9, 10 and 11)

(4) Supervisory review, tools and cooperation (Principles 12, 13 and 14)

36.10 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 risk 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.

36.11 Banks should meet all risk data aggregation and risk reporting principles simultaneously. However, trade-offs among Principles could be accepted in exceptional circumstances such as urgent/ad hoc requests of information on new or unknown areas of risk. There should be no trade-offs that materially impact risk management decisions. Decision-makers at banks, in particular the board and senior management, should be aware of these trade-offs and the limitations or shortcomings associated with them. Supervisors expect banks to have policies and processes in place regarding the application of trade-offs. Banks should be able to explain the impact of these trade-offs on their decision-making process through qualitative reports and, to the extent possible, quantitative measures.

36.12 A bank should have in place a strong governance framework, risk data architecture and information technology (IT) infrastructure. These are preconditions to ensure compliance with the other Principles included in this chapter. In particular, a bank's board should oversee senior management's ownership of implementing all the risk data aggregation and risk reporting principles and the strategy to meet them within a timeframe agreed with their supervisors.

36.13 The concept of materiality used in SRP36 means that data and reports can exceptionally exclude information only if it does not affect the decision-making process in a bank (ie decision-makers, in particular the board and senior management, would have been influenced by the omitted information or made a different judgment if the correct information had been known). In applying the materiality concept, banks will take into account considerations that go beyond the number or size of the exposures not included, such as the type of risks involved, or the evolving and dynamic nature of the banking business. Banks should also take into account the potential future impact of the information excluded on the decision-making process at their institutions. Supervisors expect banks to be able to explain the omissions of information as a result of applying the materiality concept.

36.14 Banks should develop forward looking reporting capabilities to provide early warnings of any potential breaches of risk limits that may exceed the bank's risk tolerance/appetite. These risk reporting capabilities should also allow banks to conduct a flexible and effective stress testing which is capable of providing forward-looking risk assessments. Supervisors expect risk management reports to enable banks to anticipate problems and provide a forward looking assessment of risk.

36.15 Expert judgment may occasionally be applied to incomplete data to facilitate the aggregation process, as well as the interpretation of results within the risk reporting process. Reliance on expert judgment in place of complete and accurate data should occur only on an exception basis, and should not materially impact the bank's compliance with the Principles. When expert judgment is applied, supervisors expect that the process be clearly documented and transparent so as to allow for an independent review of the process followed and the criteria used in the decision-making process.

Definitions

36.16 For the purpose of SRP36, 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.

36.17 In this chapter, the following terms should be interpreted as follows:

(1) "Accuracy" means closeness of agreement between a measurement or record or representation and the value to be measured, recorded or represented. This definition applies to both risk data aggregation and risk reports.

(2) "Adaptability" means the ability of risk data aggregation capabilities to change (or be changed) in response to changed circumstances (internal or external).

(3) "Approximation" means a result that is not necessarily exact, but acceptable for its given purpose.

(4) "Clarity" means the ability of risk reporting to be easily understood and free from indistinctness or ambiguity.

(5) "Completeness" means availability of relevant risk data aggregated across all firm's constituent units (eg legal entities, business lines, jurisdictions).

(6) "Comprehensiveness" means the extent to which risk reports include or deal with all risks relevant to the firm.

(7) "Distribution" means ensuring that the adequate people or groups receive the appropriate risk reports.

(8) "Frequency" means the rate at which risk reports are produced over time.

(9) "Integrity" means freedom of risk data from unauthorised alteration and unauthorised manipulation that compromise its accuracy, completeness and reliability.

(10) "Manual workarounds" means employing human-based processes and tools to transfer, manipulate or alter data used to be aggregated or reported.

(11) "Precision" means closeness of agreement between indications or measured quantity values obtained by replicating measurements on the same or similar objects under specified conditions.

(12) "Reconciliation" means the process of comparing items or outcomes and explaining the differences.

(13) "Risk tolerance/appetite" means 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.

(14) "Timeliness" means the availability of aggregated risk data within such a timeframe as to enable a bank to produce risk reports at an established frequency.

(15) "Validation" means the process by which the correctness (or not) of inputs, processing, and outputs is identified and quantified.

Summary of the Principles

36.18 The Principles for effective risk data aggregation and risk reporting are summarised as follows.

(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.[1]

(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.

(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.

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

(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.

(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.

(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.

(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.

(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.

(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.

(11) Distribution – Risk management reports should be distributed to the relevant parties and while ensuring confidentiality is maintained.

(12) Supervisory review – Supervisors should periodically review and evaluate a bank's compliance with the eleven Principles above.

(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.

(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.

Footnotes

[1] *For instance, the Basel Committee's Corporate governance principles for banks (July 2015).*

Principle 1 – Governance

36.19 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.

36.20 A bank's board and senior management should review and approve the bank's group risk data aggregation and risk reporting framework and ensure that adequate resources are deployed.

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

(1) Fully documented and subject to high standards of validation. This validation should be independent and review the bank's compliance with the Principles in this document. The primary purpose of the independent validation is to ensure that a bank's risk data aggregation and reporting processes are functioning as intended and are appropriate for the bank's risk profile. Independent validation activities should be aligned and integrated with the other independent review activities within the bank's risk management program,[2] and encompass all components of the bank's risk data aggregation and reporting processes. Common practices suggest that the independent validation of risk data aggregation and risk reporting practices should be conducted using staff with specific IT, data and reporting expertise.[3]

(2) 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.

(3) 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 particular, risk data aggregation capabilities should be independent from the choices a bank makes regarding its legal organisation and geographical presence.[4]

Footnotes

[2] *In particular the so-called "second line of defence" within the bank's internal control system.*

[3] *Furthermore, validation should be conducted separately from audit work to ensure full adherence to the distinction between the second and third lines of defence, within a bank's internal control system. See, inter alia, Principles 2 and 13 in the Basel Committee's Internal Audit Function in Banks (June 2012).*

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

36.22 A bank's senior management should be fully aware of and understand the 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). Senior management should ensure that the bank's IT strategy includes ways to improve risk data aggregation capabilities and risk reporting practices and to remedy any shortcomings against the Principles taking into account the evolving needs of the business. Senior management should also 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.

36.23 A bank's board is responsible for determining its own risk reporting requirements and should be aware of limitations that prevent full risk data aggregation in the reports it receives. The board should also be aware of the bank's implementation of, and ongoing compliance with the Principles.

Principle 2 – data architecture and IT infrastructure

36.24 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.

36.25 A bank should establish integrated[5] 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.

Footnotes

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

36.26 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.

Principle 3 – accuracy and integrity

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

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

(2) 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.

(3) Risk data should be reconciled with bank's sources, including accounting data where appropriate, to ensure that the risk data is accurate.

(4) A bank should strive towards a single authoritative source for risk data per each type of risk.

(5) 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.

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

36.29

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.

36.30 Supervisors expect banks to document and explain all of their risk data aggregation processes whether automated or manual (judgment-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.

36.31 Supervisors expect banks to measure and monitor the accuracy of data and to develop appropriate escalation channels and action plans to be in place to rectify poor data quality.

Principle 4 – completeness

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

36.33 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.

36.34 Supervisors expect banks to produce aggregated risk data that is complete and to measure and monitor 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' data to be materially complete, with any exceptions identified and explained.

Principle 5 – timeliness

36.35 A bank's risk data aggregation capabilities should ensure that it is able to produce aggregate risk information on a timely basis to meet all risk management reporting requirements.

36.36 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 stress/crisis situation. Banks need to build their risk systems to be capable of producing aggregated risk data rapidly during times of stress /crisis for all critical risks.

36.37 Critical risks include but are not limited to:

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

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

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

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

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

36.38 Supervisors will review that the bank specific frequency requirements, for both normal and stress/crisis situations, generate aggregate and up-to-date risk data in a timely manner.

Principle 6 – adaptability

36.39 A bank's risk data aggregation capabilities should be flexible and adaptable to meet ad hoc data requests, as needed, and 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.

36.40 Adaptability includes:

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

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

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

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

36.41 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[6] 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.

Footnotes

[6] *Including, for instance, sovereign, bank, corporate and retail exposures.*

Principle 7 – accuracy

36.42 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.

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

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

(2) 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

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

36.44 Approximations are an integral part of risk reporting and risk management. Results from models, scenario analyses, and stress testing are examples of approximations that provide critical information for managing risk. While the expectations for approximations may be different than for other types of risk reporting, banks should follow the reporting principles in SRP36 and establish expectations for the reliability of approximations (accuracy, timeliness etc) to ensure that management can rely with confidence on the information to make critical decisions about risk. This includes principles regarding data used to drive these approximations.

36.45

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

36.46 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

36.47 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).

36.48 Reports should identify emerging risk concentrations, provide information in the context of limits and risk appetite/tolerance and propose 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.

36.49 Supervisors expect banks to determine risk reporting requirements that best suit their 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.

36.50 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 and usefulness

36.51 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.

36.52 Reports should include an appropriate balance between risk data, analysis and interpretation, and qualitative explanations. 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.

36.53 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).

36.54 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 fulfil 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 tolerance/appetite.

36.55 The board should alert senior management when 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 tolerance/appetite. The board should indicate whether it is receiving the right balance of detail and quantitative versus qualitative information.

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

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

36.58 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.

36.59 Supervisors expect a bank to confirm periodically with recipients that the information aggregated and reported is relevant and appropriate, in terms of both amount and quality, to the governance and decision-making process.

Principle 10 – frequency

36.60 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 stress/crisis situations. A bank should routinely test its ability to produce accurate reports within established timeframes, particularly in stress/crisis situations.

36.61 Supervisors expect that in times of stress/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

36.62 Procedures should be in place to allow for rapid collection and analysis of risk data and timely dissemination of reports to all appropriate recipients. This should be balanced with the need to ensure confidentiality as appropriate.

36.63 Supervisors expect a bank to confirm periodically that the relevant recipients receive timely reports.

Principle 12 – supervisory review

36.64 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.

36.65 Supervisors should draw on reviews conducted by the internal or 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 or independent experts from the bank, when appropriate.

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

Principle 13 – remedial actions and supervisory measures

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

36.68 Supervisors should have a range of tools at their disposal to address material deficiencies in a bank's risk data aggregation and reporting 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.

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

36.70 For new business initiatives, supervisors may require that banks' implementation plans ensure that robust risk data aggregation is possible before allowing a new business venture or acquisition to proceed.

36.71 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

36.72 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. Wherever possible, supervisors should avoid performing redundant and uncoordinated reviews related to risk data aggregation and risk reporting.

36.73 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 Principles for effective supervisory colleges.[7]

Footnotes

[7] *See www.bis.org/publ/bcbs287.htm .*

36.74 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.