BANK FOR INTERNATIONAL SETTLEMENTS

FSI Connect
Financial Stability Institute

Risk data aggregation and risk reporting – Executive Summary

The 2007–09 Great Financial Crisis exposed severe deficiencies in the management information systems (MIS) of many of the major global banks. Certain banks took entire days, or longer, to aggregate their exposures to single counterparties. In practice, such information was needed during the crisis several times a day for multiple counterparties. Even during non-crisis episodes, such information is needed for management to make sound business decisions and for supervisors to effectively protect the safety and soundness of the financial system. The crisis therefore served as a "wake-up call" for the banking industry and the regulatory community and highlighted the need to overhaul the risk data aggregation capabilities and risk reporting practices of banks.

As a result, in 2011, the Financial Stability Board recommended the development of a set of supervisory expectations to move data aggregation capabilities of financial firms – particularly significantly important ones – to a level where supervisors, firms and other users of the data (eg resolution authorities) can be confident that the MIS reports accurately capture the risks. Subsequently, the Basel Committee on Banking Supervision (BCBS) established the *Principles for effective risk data aggregation and risk reporting* (the Principles) in 2013.

Objectives

The Principles aim 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 its ability to manage the risk of new products and services.

For bank supervisors, the Principles 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.

The Principles

The Principles are broken down into four complementary sets:

- governance and infrastructure;
- risk data aggregation capabilities;
- risk reporting practices; and
- supervisory review.

The BCBS has acknowledged that there are interactions and relationships between the Principles. For instance, poor data governance and information technology infrastructure can have a negative impact on a

bank's risk data aggregation capabilities. This, in turn, can negatively affect the quality and the timeliness of risk reporting.

The table outlines expectations in these areas.

	Expectations
Governance and infrastructure	
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 BCBS.
Data architecture and IT infrastructure	A bank should design, build and maintain data architecture and IT infrastructure that fully support its risk data aggregation capabilities and risk reporting practices, not only in normal times but also during stress or crisis.
Risk data aggregation capabilities	
Accuracy and integrity	A bank should be able to generate accurate and reliable risk data to meet normal and stress/crisis reporting requirements. Data should be aggregated on a largely automated basis to minimise the probability of errors.
Completeness	A bank should be able to capture and aggregate all material risk data across the banking group. Data should be available by different groupings (eg business line, legal entity, asset type, industry, region) relevant to the risk in question, to enable the identification and reporting of risk exposures, concentrations and emerging risks.
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, its criticality to the overall risk profile of the bank and frequency requirements for risk management reporting, under both normal and stress/crisis situations.
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, due to changing internal needs and to meet supervisory queries.
Risk reporting practices	
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.
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.
Clarity and usefulness	Risk management reports should communicate information in a clear and concise manner. Reports should be easy to understand yet comprehensive enough to facilitate informed decision-making. Reports should include meaningful information tailored to the needs of the recipients.
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.
Distribution	Risk management reports should be distributed to the relevant parties while ensuring confidentiality is maintained.
Supervisory review	
Review	Supervisors should periodically review and evaluate a bank's compliance with the 11 principles above.
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 of the Basel Framework.
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.

Implementation

The Principles apply to global systemically important banks (G-SIBs) on both a banking group and solo basis. National supervisors are strongly encouraged to apply the Principles to their domestic systemically important banks as well. They may also choose to apply them to a wider range of banks in a way that is proportionate to the size, nature and complexity of their operations.

G-SIBs were expected to meet the Principles in 2016. The BCBS implementation monitoring has observed tangible progress over the years in several key areas, including governance, risk data aggregation capabilities and reporting practices. However, the 2020 BCBS report noted that none of the G-SIBs has achieved full compliance with the Principles, as attaining the necessary data architecture and IT infrastructure remains a challenge for many.

This Executive Summary and related tutorials are also available in FSI Connect, the online learning tool of the Bank for International Settlements.