Finalyse

A fresh take on
risk and valuation

Memo

BCBS 239

Principles for Effective Risk Data Aggregation and Risk Reporting
November 2016

Summary

Set of 14 principles to strengthen banks' risk data aggregation capabilities and internal risk reporting practices in reaction to shortcomings in risk management, which became evident during the crisis. It aims at creating a robust data framework for G-SIBs:

- Date of adoption: January 2013
- Date of application: Banks identified as G-SIBs by the FSB (Nov 2011 or 2012) must comply by January 2016, later identified G-SIBs must comply three years after their identification.
- Concerns: Banks

1. Scope

- Apply to **SIBs** at both the banking group level and on a solo basis
  - G-SIBs obligatory, D-SIBs should be forced by national supervisor
  - National supervisors can choose to apply it to a wider range of banks
- Apply to **all key internal risk management models**, including Pillar 1 and 2 capital models and other key risk management models (eg value-at-risk)
- Apply to a bank's **group risk management processes**
  - Also to **outsourced** processes
  - Applying them to other processes, such as financial and operational processes, and supervisory reporting can be beneficial for banks
- Risk data aggregation and risk reporting principles have to be met simultaneously
  - Unless a trade-off is present, then internal policies must regulate it

Key question for implementation: What are the costs and benefits for applying BCBS 239 to an extended scope of processes?

2. The Principles

BCBS 239 consists of **14 principles** in four categories, of which **11 for banks** and 3 for supervisors:

1. Overarching governance and infrastructure

A bank should have in place a strong governance framework, risk data architecture and IT infrastructure.

1. Principle 1: 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.
2. Principle 2: 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.

2. Risk data aggregation capabilities

Banks should develop and maintain strong risk data aggregation capabilities to ensure that risk management reports reflect the risks in a reliable way.

3. Principle 3: 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. Principle 4: 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. Principle 5: 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. Principle 6. 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.

3. Risk reporting practices

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.

7. Principle 7: 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. Principle 8: 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. Principle 9: 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.
10. Principle 10: 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. Principle 11: Risk management reports should be distributed to the relevant parties while ensuring confidentiality is maintained.

4. Supervisory review, tools and cooperation

Supervisors should review compliance with the Principles to determine whether the Principles themselves are achieving their desired outcome and whether further enhancements are required.

12. Principle 12: Supervisors should periodically **review and evaluate** a bank's compliance with the eleven Principles above.
13. Principle 13: 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. Principle 14: 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.

References

- BCBS 239 http://www.bis.org/publ/bcbs239.pdf
- EY briefing http://www.ey.com/Publication/vwLUAssets/EY-bcbs-239-risk-data-aggregation-reporting-AU/%24FILE/EY-bcbs-239-risk-data-aggregation-reporting-AU.pdf
- McKinsey briefing https://www.google.be/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwj7hMOc9JjQAhWrJsAKHd8pBRAQFggdMAA&url=http%3A%2F%2Fwww.mckinsey.com%2F~%2Fmedia%2FMcKinsey%2Fdotcom%2Fclient_service%2FRisk%2FPDFs%2FCapturing%2520value%2520from%2520BCBS%252020239%2520and%2520beyond.ashx&usg=AFQjCNHpvU-68Ld2RZz2XspatXZIRjURQg