Risk and Regulation

It's not just about getting your ratios right

Basel's far-reaching new risk IT requirements

January 2013
Keiichi Aritomo
Tommaso Cohen
Philipp Härle
Holger Harreis
Kayvaun Rowshankish
Hamid Samandari

It's not just about getting your ratios right: Basel's far-reaching new risk IT requirements

Introduction

The Basel Committee on Banking Supervision (BCBS) has issued a new regulation on risk aggregation and reporting that significantly increases the risk IT capabilities banks must have and sets an aggressive timeline. Our analysis of the new rule yields several insights. It now appears that a unified set of global and local regulations on risk IT is out of reach; that the new rule sets a very high bar for banks; that the regulation will prompt some serious decisions that must be taken at the bank's highest level; and that compliance is likely to be difficult, with severe sanctions for failure.

With so much to do, banks may be at a loss about how to begin. We see five priorities for immediate action: engage with supervisors to detail the implementation requirements, adapt the risk IT governance model, ensure the compliance effort is properly resourced, develop an action plan to coordinate the effort, and start now, as time is of the essence.

That action plan is the centerpiece of the effort. To help banks think it through, we conclude with a discussion of the core elements that are likely to be included in most bank's plans, beginning with a risk IT diagnostic, to understand the current level of capability.

The stakes have been raised: New requirements for risk IT and operations

Risk IT and operations have moved rapidly up the regulatory agenda in the past few years. The Financial Stability Board (FSB) and Senior Supervisors Group, in addition to the BCBS, have focused their attention on the topic.[1] The industry, led by the Institute of International Finance and supported by McKinsey, provided a response and proactively engaged in the public debate through the report *Risk IT and Operations: Strengthening Capabilities*, published in June 2011.[2]

Now, BCBS Regulation 239, on principles for effective risk aggregation and risk reporting,[3] sets out the first global regulation directly relevant to risk IT and operations. Today's global systemically important banks (G-SIBs, also known as G-SIFIs) must comply by January 1, 2016; banks designated as G-SIBs at a later date will have to be compliant three years after that designation is made. The BCBS is encouraging local authorities to apply similar requirements in a similar timeframe to domestically important banks (D-SIBs) and in proportion to a wider range of banks.

The regulation is principles-based and sets high standards to make risk aggregation and reporting more timely, more accurate, more comprehensive, and more granular. It covers internal reporting, not regulatory reporting, and sets out principles in four key areas:

Governance and infrastructure. The regulation calls for risk governance to encompass risk-data aggregation and reporting, and it says that systems designed for risk aggregation and reporting should function well under stress or crisis.

Data-aggregation capabilities. The rule raises the bar for data and data processes. Banks must be able to provide highly automated aggregation with minimal manual intervention; data must be available by "business line, legal entity, asset type, industry, (and) region." Data aggregation must be current and timely, and the process must be adaptable and flexible, enabling ad hoc requests.

Reporting practices. Here, too, the regulation calls for higher standards. Reports must be accurate, reconciled, and validated; comprehensive, covering each domain; clear and tailored to the audience; and generated and distributed in a way that is appropriate for the audience and context.

Supervisory review and cooperation. Regular supervisory review of risk aggregation and reporting calls for supervisors to require effective and timely remedial action; they can use Pillar 2 measures and set limits on banks' risks and growth; and it says that home and host supervisors should cooperate on reviews. Specific implementation requirements and action plans based on these principles will be discussed and detailed with supervisors for each individual bank, commencing in spring 2013. As part of this process, firms will have to complete a self-assessment for supervisors, the results of which will be included in a joint FSB–BCBS report.

1 See *Observations on Developments in Risk Appetite Frameworks and IT Infrastructures*, Senior Supervisors Group, December 2010 (newyorkfed.org), and *Intensity and Effectiveness of SIFI Supervision: Progress Report on Implementing the Recommendations on Enhanced Supervision*, Financial Stability Board, October 2011 (financialstabilityboard.org).
2 This report is available on mckinsey.com and iif.com.
3 See *Principles for Effective Risk Aggregation and Risk Reporting*, Bank for International Settlements, January 2013 (bis.org).

We see several key insights emerging from this for banks:

Global standards for risk IT and operations are unlikely. Banks might well face multiple compliance needs, as the BCBS regulation is pitched at a high level and the process to shape home and host supervisor cooperation has not been clearly established.

Some new standards are far-reaching and well beyond banks' current capabilities. Each principle on its own formulates a reasonable aspiration and can help to improve a bank's capabilities significantly. But some go beyond this to set requirements that, in light of banks' current capabilities, will be exceptionally challenging to meet. These highly aspirational requirements include the competing demands of frequency versus accuracy and comprehensiveness of reports in times of stress, the level of automation in reconciliations, and the depth of senior-management and board involvement expected in the tight time frame, especially given other investment needs imposed on banks.

Risk aggregation reaches the top levels of the bank's organization and influences strategic decisions. Risk aggregation and risk IT is now a topic for senior management and the board, particularly because it is now relevant to strategic decisions such as M&A, new strategic initiatives, and new products; it is also important because of the significant decisions that must be made with respect to the trade-offs among quality, limitations, and other factors.

The consequences of noncompliance are severe. Regulators have set up significant penalties for noncompliance, including capital add-ons under Pillar 2 and limits on risks and growth.

What will compliance look like?

While the ink on the new regulation is barely dry, many banks are naturally curious to understand what their risk IT aggregation and reporting infrastructure will need to look like to be compliant with the new regulation. The exhibit provides a few examples, which make clear how challenging it will be to achieve the new standards.

Exhibit New regulation will drive changes in banks' risk IT/operations capabilities.

EXAMPLES: NOT EXHAUSTIVE

	From…	To…
Governance and infrastructure	▪ Accountability spread across functions and levels; risk IT not considered a strategic asset	▪ Clear unified accountability from top management through the organization ▪ Risk-aggregation capabilities factored into strategic decisions
Data-aggregation capabilities	▪ Multiple data models and data taxonomies across legal entities and risk types	▪ Unique or more consolidated data models and taxonomies across the institution
	▪ Big portion of risk aggregation done manually, "off the systems" (eg, Excel models)	▪ Automatic, high-frequency aggregation within the standard systems space
	▪ Counterparty-risk calculation available at front office at T+1 4pm	▪ Counterparty-risk calculation available at T+1 8am—even in times of market stress
Reporting practices	▪ Reporting from multiple systems with rigid, standardized reports with predefined frequencies	▪ Standard reporting more tailored for audience (both contents and timing) ▪ Need to produce in near real time "on-demand reports" for specific risk type (eg, market and counterparty) for specific audience (eg, traders)
Supervisory review and cooperation	▪ Risk IT at the edge of the radar screen of many supervisors	▪ Regulators will need to sign off on risk IT infrastructure before M&A deal is approved

Business benefits

Our experience also suggests that banks can capture significant business benefits beyond regulatory compliance:

- Lower losses because of better data quality and superior risk insights: losses can be lowered by 2 to 4 percent.
- Lower capital needs because of more accurate categorizations and more frequent updates: one bank, for example, was able to eliminate its $7 billion Financial Services Authority–mandated liquidity buffer, which carried an estimated 4 percent opportunity cost.
- Lower operational risk costs because of less manual effort and better fraud detection: banks can save 5 to 10 basis points currently lost to fraud.
- Lower operational costs because of better data management and reduced number of reconciliations: banks can save 5 to 10 percent of some big operational-cost categories.

Compliance will require a major effort. Given the numerous high standards and in light of the timeline, banks are facing a major transformation challenge. (See "What will compliance look like?" below.) However, in our experience, banks should view this as an opportunity. A comprehensive risk IT/operations transformation can bring tangible business benefits (reduced losses, lower capital needs, lower operational costs, and improved risk-adjustment capabilities) if consistently focused on business value. "Business benefits" above provides more detail.

Five priorities for immediate action

Based on the above, we believe the regulation calls out five important priorities for firms to act on today:

1. Engage with supervisors. Banks need to invest in working with their home supervisor to define an action plan that translates the principles into specific requirements. In parallel, banks should engage with host regulators in other countries where they are active, to ensure cooperation and align on the action plan.

2. Define an action plan. Banks should proactively translate principles into specific requirements to define the minimum set of capabilities needed for compliance. In doing so, they should pay special attention to making sure to address real business value with these compliance requirements. (See below for key elements that might be included in the action plan.)

3. Adapt governance. Banks need to review and likely adapt risk governance and culture across the organization to extract value from better risk aggregation. Strategic decision-making processes should be revisited to include risk-aggregation and risk IT capabilities.

4. Ensure compliance. Compliance implementation needs to be resourced with top talent and clear responsibility assigned to senior managers. Compliance needs to be continuously monitored and incentivized.

5. Start now. Banks should find a pragmatic approach to implementation that minimizes cost while reaping as much business value as possible. As suggested by the BCBS, banks need to act now if they are to be compliant by the beginning of 2016.

A comprehensive action plan

Our experience helping banks deliver risk IT programs suggests that a comprehensive action plan will include the following five steps. The extent of the effort in each of the final four steps will depend on the maturity of the bank's capabilities:

1. Conduct a rapid risk IT diagnostic. Banks should use industry best practices, internal standards, and regulatory principles to assess their current capabilities and identify and prioritize gaps.

2. Design effective governance and data policies. Banks need a risk IT governance model that defines accountability, a set of clear decision-making processes, participation from business and senior leadership, and engagement with stakeholders (including regulators). Data policies should include measurable standards for completeness, accuracy, and frequency; roles and responsibilities should be defined across the data life cycle.

3. Build the data model and architecture. Banks must develop data requirements, including definitions of attributes,

hierarchies, and taxonomies; they must also establish an ongoing process, metrics and targets to ensure data quality. Where appropriate, they should clean their data, using a phased process based on defined measures and risk/benefit prioritization. With the business as a partner, risk IT groups should design the data model (including conceptual and logical models, covering transactional and reference data). And they must design the data architecture (operational and informational) and technical architecture, conforming to best-practice separation of layers (for example, storage versus business rules).

4. Establish data aggregation and analytics capabilities. Banks will want to develop aggregation, reporting, and analytics requirements using proofs of concept and "wireframes" to iterate and align with risk and business user needs. As they design the technical architecture, they should identify key modules that best serve the analytics and aggregation requirements of the firm to help make the best buy-versus-build decisions.

5. Create a project-management office (PMO) and implement. Banks should set up a PMO to manage the risk IT transformation, with focus on managing value delivery, providing clear communications, and establishing accountability. To implement the program, banks should develop a risk IT transformation roadmap that sets out milestones for incremental releases that will demonstrably advance the capture of benefits.

In this article, we have attempted to distill a great deal of information in a limited space to help banks sort out the implications of the new rule. If we had to take that logic to an extreme, we would urge banks to do two things: take on the first priority we listed, and proactively engage with home and host supervisors to align on the approach. Banks cannot afford to go it alone. Second, they should take that first step in the action plan, and conduct a quick assessment to calibrate their current capabilities against the regulation principles. Banks cannot proceed without knowing where they currently stand.

Keiichi Aritomo is a principal in McKinsey's Tokyo office, **Tommaso Cohen** is an associate principal in the Milan office, **Philipp Härle** is a director in the London office, **Holger Harreis** is a principal in the Düsseldorf office, and **Kayvaun Rowshankish** is a principal in the New York office, where **Hamid Samandari** is a director.

Risk and Regulation
January 2013
Designed by Global Editorial Services design team