



PROMONTORY

Sightlines

IN FOCUS

promontory.com

JUNE 30, 2015

BY RAY STRECKER, YOKO OTANI, AND STACY COLEMAN

Better Risk Data: Regulatory Mandate and Strategic Opportunity



Ray Strecker
Managing Director

At the heart of the sustained effort to improve risk management at financial institutions is better information — and the ability to assess and manage it quickly. Managing risk information well has become a strategic advantage for institutions expanding into new markets and developing new products, and an essential component in meeting regulatory expectations.

Regulators' interest in risk information is mounting. Most recently, the Financial Stability Oversight Council identified data limitations as potential emerging threats and vulnerabilities to financial stability, stating that "critical gaps remain in the scope, quality, and access to data."¹ The Basel Committee on Banking Supervision issued principles-based guidance in 2013 for risk-data aggregation and reporting (RDAR), formally requiring that the largest banks build and maintain capabilities sufficient to assess risks in normal and stressed markets.²



Yoko Otani
Managing Director

These initiatives are meant to ensure better information for boards and executive management, regulators, market participants, and investors. Banks and other affected institutions have invested significantly to meet these requirements. Despite these efforts, the FSOC report, combined with a BCBS report issued in January³ describing progress on RDAR at the 37 largest banks, suggests that the industry still has much work to do.



Stacy Coleman
Senior Director

Many banks are attempting to meet specific deadlines — for the Dodd-Frank Act stress tests (DFAST), the Federal Reserve FR Y-15,⁴ and Basel III compliance — by building a series of one-off processes and systems to address each requirement. The emphasis on expediency is understandable considering the time pressures, but that approach can lead to a patchwork of partial capabilities that are not readily adaptable to new requirements or regulatory and market needs, are difficult to keep in synch, and are often extremely expensive to operate and maintain. A set of one-off systems that meet each specific requirement individually may worsen inconsistencies and actually leave the bank

¹ <http://www.treasury.gov/initiatives/fsoc/studies-reports/Documents/2015%20FSOC%20Annual%20Report.pdf>

² <http://www.bis.org/publ/bcbs239.pdf>

³ <http://www.bis.org/bcbs/publ/d308.pdf>

⁴ http://www.federalreserve.gov/reportforms/forms/FR_Y-1520131231_i.pdf. This report collects consolidated systemic-risk data from large U.S. bank holding companies. The data items collected in this report mirror those developed by the Basel Committee on Banking Supervision to assess the global systemic importance of banks.

farther away from having the authoritative, consistent information it needs to satisfy the BCBS principles and to be confident in its information when facing a crisis.

Instead, banks and other financial institutions should aim for a comprehensive approach to managing risk information that not only satisfies regulatory requirements, but also supports use of the information to make better-informed strategic decisions. Getting a firmer grasp on developing risk-information requirements — and opportunities — will help board members, chief executive officers, and business leaders gauge the long-term health of their banks' business.

Background: Regulatory Developments Related to Risk Data

The global financial crisis exposed flaws in the resources that many institutions relied upon to understand their risks. Since then, financial institutions — particularly large banks — have faced increasing regulatory demands to produce risk information in the form of reporting or data-intensive modeling. For example:

- Systemic-risk reporting through the FR Y-15
- DFAST
- Comprehensive Capital Analysis and Review (CCAR), including the FR Y-14 monthly, quarterly, and annual reporting requirements
- Resolution planning
- The Federal Reserve's Liquidity Monitoring Report (FR 2052b)
- Basel III risk-weighted asset calculations
- Bank for International Settlements data hub reporting for global systemically important banks (G-SIBs)

Regulators have also launched initiatives focused on improving the transparency of various markets by helping regulators, market participants, and investors see buildups of concentrations and other signs of trouble. The FSOC report discusses efforts to establish common legal-entity identifiers (LEIs) for use across financial markets, the development of universal loan identifiers for the housing market, data-collection efforts in repurchase (repo) markets, and enhanced data collection for swap data repositories.

Each year, regulators raise their expectations for the quality of data and analysis supporting stress testing and resolution planning. They also continue to issue new requirements — for example, reporting on liquidity coverage ratios (LCRs) — and develop market-specific initiatives.

The BCBS principles related to risk-information management may prove even more significant in the long run. By requiring governance at the highest levels of the organization, the principles elevate the quality of risk information to a board-level topic and require board attention to RDAR as part of its oversight of the risk management framework. The principles are directly applicable to G-SIBs, the world's 31 largest institutions, which are expected to comply with the 11 principles within the guidance by January 2016. Local regulators are encouraged to apply the same principles to other large institutions in their respective jurisdictions.

The Office of the Comptroller of the Currency's heightened standards for risk management in large U.S. institutions identify risk-data aggregation and reporting as an explicit element, and cite the RDAR principles.⁵ The OCC's statement of requirements related to risk data, shown in Figure 1 below in its entirety, is brief, but clearly echoes key themes in the more extensive BCBS principles.

Given the brevity of the OCC statement, banks covered by heightened standards should look to the BCBS principles and the programs undertaken by institutions already subject to those principles as the benchmark for assessing their own capabilities and developing action programs. The principles offer comprehensive guidance for all financial institutions in reviewing the quality of their risk information.

Meeting these expectations is crucial. The Federal Reserve has specifically cited weaknesses in management information systems and risk identification, measurement, and aggregation as reasons why some banks failed to meet CCAR's qualitative requirements. That, in turn, required banks to amend their capital plans. Regulators have also pointed to the inability to "produce reliable information in a timely manner" as one of the major shortcomings in banks' resolution plans.⁶

Since the financial crisis, U.S. regulators have consistently emphasized the importance of forward-looking, data-driven assessments as a critical part of their supervisory programs. Now that U.S. regulators have issued many of their reforms on capital and liquidity, they will begin to focus more heavily on the implementation of those reforms, including the quality of data and systems that support implementation.

⁵ <http://www.occ.gov/news-issuances/news-releases/2014/nr-occ-2014-4a.pdf>

⁶ See <http://www.federalreserve.gov/newsevents/press/bcreg/20140805a.htm>.

FIGURE 1. EXPECTATIONS AND PRINCIPLES

The OCC's final rule on heightened expectations spelled out requirements for risk-data aggregation and reporting that are similar to the more in-depth principles issued by the Basel Committee on Banking Supervision that offer appropriate benchmarks for financial institutions.

U.S. OCC Heightened Standards

Risk-data aggregation and reporting. The risk-governance framework should include a set of policies, supported by appropriate procedures and processes, designed to provide risk-data aggregation and reporting capabilities appropriate for the size, complexity, and risk profile of the covered bank, and to support supervisory reporting requirements.

Collectively, these policies, procedures, and processes should provide for:

1 The design, implementation, and maintenance of a data architecture and information technology infrastructure that support the covered bank's risk-aggregation and reporting needs during normal times and during times of stress.

2 The capturing and aggregating of risk data and reporting of material risks, concentrations, and emerging risks in a timely manner to the board of directors and the OCC.

3 The distribution of risk reports to all relevant parties at a frequency that meets their needs for decision-making purposes.

BCBS Principles of Effective Risk-Data Aggregation and Reporting

A bank's risk-data aggregation capabilities and risk-reporting practices should be subject to strong governance arrangements.

A bank's risk-data aggregation and reporting processes are functioning as intended and are appropriate for the bank's risk profile.

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.

A bank should be able to generate aggregate and up-to-date risk data in a timely manner.
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.

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.

Challenges in Managing Risk Data

The BCBS principles state that “controls surrounding risk data should be as robust as those applicable to accounting data.” Achieving this goal is not easy. Consider two brief anecdotes:

- A bank building its auto-lending portfolio wanted to analyze loan-to-value ratios for its book of business. Even though its systems captured a vehicle description, they did not routinely include the vehicle make, model, and year — information needed to support the analysis. The bank undertook an expensive, manual exercise to collect and enter the data from original loan documents.
- A bank with a global funds-transfer and trade-finance business needed to assess the anti-money-laundering and sanctions compliance risks posed by its network of international correspondent banks. The bank approached the exercise believing its existing customer data, which identified customers based on an LEI scheme, would be adequate. The bank found it could not readily associate transactions to specific correspondent branches in higher-risk countries because banks typically have a single LEI for their head office and all their branches.

Generalizing a bit, there are several reasons why risk data is hard to manage and control:

- 1. Most risk data is not accounting data and may be difficult to control in the same way.** A mortgage-risk report, for example, will likely show some accounting data (e.g., outstanding principal balance), but it might also show tenor, rate terms, LTVs, credit scores, recourse, and many other facts that bear on risk. These elements may all be in the bank’s loan-accounting systems, but they are not subject to the rules of double-entry bookkeeping and may not be easily reconciled to general ledger balances. Controlling their accuracy, especially in reports that assemble data from multiple loan-product systems, may not be straightforward.
- 2. Data collected for other purposes may not be adequate for risk.** In the anecdotes above, we saw vehicle descriptions that were adequate for loan operations and customer identifiers adequate for relationship management, but neither was adequate for risk analysis. Similarly, reports on product volume and other trends may not capture specific terms important in determining whether a portfolio’s risk profile is changing.
- 3. Risks evolve and information needs to evolve with them.** Operational risk, in particular, is a source of expanding risk and uncertainty for the industry. For example, the continuous migration of financial transactions to electronic channels and the growing sophistication of hackers are increasing both the likelihood and the impact of cybersecurity losses. Historical loss data is not likely to be a good predictor of future exposure.

Many financial institutions have significantly improved their reporting to senior management and the board. In spite of these advances, putting the numbers together for top-of-the-house reporting often remains labor-intensive, at the expense of thoughtful analysis and commentary.

To control and manage risk data properly, financial institutions need to draw on a broad set of approaches and tools, particularly if the starting point is a patchwork of single-purpose reporting systems integrated through back-end spreadsheets. Three pillars of effective risk-data management simplify this complex topic:

- 1. Appropriate business engagement.** The business must define its risk-data needs, and must take ultimate responsibility for ensuring data quality. This includes rules for source data and aggregation — for instance, in calculating capital under different definitions. The IT organization can work with the business to tackle these problems but cannot solve them by itself.
- 2. Strong IT architecture.** Effective risk-data management in a large organization requires significant investment in modern tools: centralized data-warehouse tools, local data marts to support various user communities, and master data-management tools to establish reliable systems of record for customer information, product information, and transaction histories. Increasingly, the technical infrastructure also includes big-data tools for analyzing unstructured information such as contract terms negotiated deal by deal.
- 3. A committed data-governance program.** Tools are only as good as the data they contain. Data governance is the overall process of defining the roles of the business, operations, and technology in specifying data, capturing it accurately, aggregating it properly, and managing its quality to enable effective use. Increasingly, organizations appoint a chief data officer to manage data governance at an enterprise level. To be effective, a CDO must have the attention and support of top executives to obtain funding, gain cooperation, and drive accountability.

Banks that have made successful investments in data-quality programs and tools for other purposes, including customer relationship management, will likely find they have a head start on managing risk data. Because maintaining a fragmented, labor-intensive, and inconsistent infrastructure is expensive, a data-governance program that includes consolidation and modernization of the IT architecture will often have a compelling cost-saving business case, in addition to its regulatory and strategic justification.

Progress on Risk-Data Aggregation and Reporting

Many financial institutions have significantly improved their reporting to senior management and the board. In spite of these advances, putting the numbers together for top-of-the-house reporting often remains labor-intensive, at the expense of thoughtful analysis and commentary.

Banks generally have made significant investments in the underlying infrastructure for risk information; the BCBS progress reports cite significant IT infrastructure and architecture projects at G-SIBs. Many other banks have launched data-governance programs and significant MIS projects with improved risk information as a primary goal. Programs can exceed \$100 million.

Banks have relied upon these investments to meet new requirements for reporting and stress testing, but not with uniform success. In a recent press release, the Federal Reserve noted that four firms participating in the most recent DFAST submitted incorrect data that required remediation. As noted previously, the Federal Reserve has also cited insufficient MIS when objecting to capital plans related to CCAR.

Complying with particular reporting or modeling requirements may not be easy, but it has proven easier than complying with the broad principles articulated by the BCBS and the OCC — and it seems that banks are increasingly aware of the challenges they face.

According to the BCBS 2014 progress report released in January, 14 of 30 G-SIBs reported that they do not expect to meet the January 2016 deadline for full compliance; in the prior year's survey, only 10 of those banks said they did not expect to meet the deadline. On specific principles related to data architecture and IT infrastructure, accuracy and integrity of data aggregation, and accuracy of reporting, more banks downgraded than upgraded their assessment of readiness compared to a year ago. The report attributes the trend to banks' increased understanding of all that remains to be done, despite considerable efforts, noting that many banks are funding multiple, large IT projects.

The report also expresses concern that some aspects of the banks' self-assessments may be "overly ambitious." The banks as a group rate themselves higher on principles related to reporting practices than on principles related to governance, infrastructure, and aggregation, even though the BCBS views the latter three as prerequisites to compliance with the reporting principles. The report expressed concern that "heavy reliance on manual processes and interventions to create risk reports" could limit the banks' ability to produce accurate and timely information in a period of crisis or stress.

Obtaining information on progress at banks that are not G-SIBs is more difficult, but six additional banks below the G-SIB level participated in the 2014 survey and reported readiness similar to that of the larger institutions.

FIGURE 2. PROGRESSION IN RISK-DATA MANAGEMENT

Questions	Additional Considerations
<p>1 Does the board risk committee's (or top management's) risk package provide a clear and comprehensive picture of our risks and the actions we are taking to manage them?</p> <p>Can the firm produce reliable, informative, effective, and timely reports for all stakeholders (board, management, day-to-day users, and supervisors)?</p>	<ul style="list-style-type: none"> Does the reporting package cover all risk types, including operational, model, and liquidity risks for the institution as a whole — not just credit risk and concentrations? Do our reports link actual risk to risk appetite, indicating any limit breaches, trends threatening limits, and corresponding corrective actions?
<p>2 In the next crisis, will our institution be able to produce information that is as timely, accurate, and detailed as we need to manage through it?</p>	<ul style="list-style-type: none"> Are credible special reporting procedures in place for critical events and stress scenarios? When corrections occur, do they reflect updates to fast-changing situations or do they indicate underlying problems? In determining whether data is too detailed or too hard to obtain, do we consider whether it could change a business or strategic decision?
<p>3 Is the board engaged in discussion of reporting needs?</p>	<ul style="list-style-type: none"> For the banks subject to the BCBS principles, the board is required to "determine" its reporting requirements. Is our bank doing this?
<p>4 Have regulators or internal audit raised issues related to risk-data aggregation and reporting?</p>	<ul style="list-style-type: none"> If so, what is the corrective plan and its status? Is this discussed as part of regular board and executive reporting?
<p>5 Do we understand how risk-data is aggregated and reported today and what it is costing us?</p>	<ul style="list-style-type: none"> What percentage of our risk reporting, excluding commentary, comes directly from IT systems? Does each new reporting requirement result in a new permanent team to extract and manipulate data from our systems every reporting period? Have we looked at the costs and benefits of rationalizing our technology and production operation?

Questions	Additional Considerations
<p>6 Do we have a strong data-governance program with adequate focus on risk information specifically?</p>	<ul style="list-style-type: none"> Do we have a CDO and is risk data a major priority for the data-governance program? Is there ownership of aggregation rules — e.g., for what counts toward varying definitions of capital or risk-weighted assets? Is information available to meet the needs of decision-makers at each level — transactional management, executive management, and the board?
<p>7 Is there sufficient business ownership of information requirements, data quality, and prioritization of investments?</p>	<ul style="list-style-type: none"> Does the business take the time to think through our requirements and explain them to IT or are we asking IT to just "figure it out" for us? Do we have clear business ownership of data quality, starting with the entry of correct and complete data?
<p>8 Is risk information getting the right priority among our IT initiatives?</p>	<ul style="list-style-type: none"> Are we investing enough in risk information to meet our strategic needs and our regulatory expectations? Are we giving risk information visibility and investment focus comparable to what product and channel investments are given?
<p>9 How solid is our overall technology infrastructure for risk aggregation and reporting?</p>	<ul style="list-style-type: none"> Are there authoritative sources of customer, product, and exposure data that are sensitive to risk? (Technical terms for these might include "data warehouse," "data mart," and "master data-management systems.") Do the quantitative portions of reporting for top management and the board require extensive manipulations in spreadsheets or are they primarily automated? Are big-data technologies used to analyze high-volume unstructured information items such as swap contract terms or loan covenants? Are we getting information in dashboards that give us drill-down and analytic capabilities or are we still getting canned reports? (Traditional reporting is acceptable but more modern tools are indicative of upgraded infrastructure.)
<p>10 Are we steadily improving risk information for management or are we just keeping up with regulatory guidance?</p>	<ul style="list-style-type: none"> Do we have the strategic understanding of the value of risk information underlying the BCBS RDAR principles?
<p>11 Are front-line units and independent risk management using the same information sources and reviewing consistent output?</p>	<ul style="list-style-type: none"> Is energy being spent on time-consuming reconciliations of multiple ways of viewing the same information? Does our information architecture free the line businesses and risk function to focus on what to do about the facts, or are we struggling to reconcile competing versions of what the facts are?

Thoughts for Boards and Business Leaders

In raising the bar on the quality of banks' risk data and the timeliness of risk reporting, regulators are pushing banks to do what sound business practices suggest they do anyway: strengthen risk information and the technology infrastructure that produces it. Banks have found that this can be quite difficult, given the number of senior-level stakeholders who need to be involved, the operational changes that have to be made, and the technology investments required.

Board directors, line-of-business leaders, and risk executives understand the stakes, but may not find it easy to understand how their bank is progressing. Answers to the questions in Figure 2 may provide some benchmarks.

For G-SIBs, awareness of RDAR expectations and preparations to meet those expectations are already high. For U.S. banks with more than \$100 billion in assets, the RDAR requirements as defined by heightened standards are already in effect; U.S. banks with more than \$50 billion in assets should have a program in place to meet deadlines. Banks near the \$50 billion threshold may want to consider similar programs, and all banks can benefit by thinking through how these principles and the checklist questions above apply to them. Every financial institution is responsible for defining and obtaining the information needed to manage its risks.

The challenges in managing risk data may seem daunting. As with many other types of information, banks that embrace the challenge and commit to having more and better data and using it effectively can turn risk information into a strategic asset.

About the Authors

Ray Strecker is a managing director at Promontory and advises clients on large-scale program design and management at the intersection of regulation, risk, and technology.

Yoko Otani is a managing director at Promontory and advises clients on risk and compliance matters, including asset-liability and liquidity risk management issues, and helps integrate strategic and regulatory objectives.

Stacy Coleman is a senior director at Promontory, and assists clients on a variety of regulatory and supervisory issues. Previously, she represented the Federal Reserve in developing the Basel Committee on Banking Supervision's Principles of effective risk data aggregation and reporting.

Contact Promontory

For more information, please call or email your usual Promontory contact or:



Stacy Coleman

Senior Director, Washington, DC

scoleman@promontory.com

+1 202 384 1196



James Pastro

Director, New York

jpastro@promontory.com

+1 212 542 6830



Evelyn Fuhrer

Managing Director, New York

efuhrer@promontory.com

+1 212 365 6565



Ray Strecker

Managing Director, New York

rstrecker@promontory.com

+1 212 365 6980



Yoko Otani

Managing Director, New York

yotani@promontory.com

+1 212 542 6744



To subscribe to Promontory's publications, please visit promontory.com/subscribe.aspx



Follow Promontory on Twitter [@PromontoryFG](https://twitter.com/PromontoryFG)



Promontory Financial Group helps companies and governments around the world manage complex risks and meet their greatest regulatory challenges. We are the world's foremost experts in financial risk, regulation, and compliance. Former U.S. Comptroller of the Currency Eugene A. Ludwig founded Promontory in 2001.

Promontory Financial Group, LLC
801 17th Street, NW, Suite 1100, Washington, DC 20006 Telephone +1 202 384 1200 Fax +1 202 783 2924 promontory.com

© 2015 Promontory Financial Group, LLC. All Rights Reserved.