In January 2013, the Basel Committee on Banking Supervision (BCBS) issued the document *Principles for Effective Risk Data Aggregation and Risk Reporting*.

This guidance, directed to Global Systemically Important Banks (G-SIBs) and their supervisors, sets expectations regarding management and reporting of risk data. G-SIBs must adhere to these risk data aggregation and reporting (RDAR) principles by the end of 2015. The BCBS document also suggests that supervisors apply the same principles to domestic systemically important financial institutions within three years of a bank being so designated. To be clear, these principles are not currently being implemented through a regulatory compliance regime that follows the rule making process under U.S. law. As such, we expect regulatory expectations vis-à-vis these principles to be embedded in the examination and compliance processes underlying data intensive regulations such as Basel III, Comprehensive Capital Analysis and Review (CCAR), elements of the Dodd-Frank Wall Street Reform and Consumer Protection Act’s Enhanced Prudential Supervision standards, and in risk management and governance assessments.

Since the financial downturn, the focus on data has generally increased with “data centric” regulatory examinations that challenge institutions to prove data quality or reconciliation of risk data to the ledger or demonstrate traceability of information from source to final reports or vice versa. The RDAR principles continue to raise the bar with respect to regulatory data-related expectations. The RDAR principles provide regulators a structured approach to assessing the multitude of risk, capital, and regulatory requirements that should be enabled by a common enterprise data infrastructure. The new guidance also elevates the role of data in overall organization governance by recognizing board and senior management responsibilities regarding information used in their risk-related oversight capacity.

Addressing deficiencies will require a holistic approach as an institution translates capability gaps into actionable steps that impact related elements of the infrastructure. In addition, an important underlying theme of this paper is that the responsibility for identifying the metrics that are required lies with the institution’s highest officers, so the processes for enhancing risk information foundation must address this responsibility.

This paper, directed to senior banking executives, chief risk officers, and board-level and management risk committee members, examines some of the key issues raised by the RDAR principles in order to flag challenges and foster discussion and planning.

---

1 See “Principles for effective risk data aggregation and risk reporting,” Basel Committee for Banking Supervision, January 9, 2013.
The story so far
European G-SIBs appear to have responded sooner to the guidance than many U.S. banks. Some responded after the June 2012 release of the BCBS consultative paper with the same title, in expectation of regulatory contact or by initiating contacts, while others took a “wait and see” approach. After the January 2013 release of the final document, U.S. G-SIBs responded to a questionnaire from U.S. banking regulators seeking an assessment of readiness with the RDAR principles and a plan for addressing gaps by 2015. The relatively short time for U.S. banks’ assessments combined with differences in approach resulted in assessment submissions that likely do not provide a sufficient horizontal perspective to the regulators. The road maps for addressing gaps and implementing these principles will likely be refined. Also, while U.S. banking regulators are currently focused on the eight G-SIBs domiciled in the U.S., some U.S. regional banks required to comply with CCAR and the Capital Plan Review (CapPR) processes are considering the potential impact of the principles.

As noted previously, even before publication of the final guidelines, regulators had been focusing on the quality of risk data, its consistency with financial data, and the robustness of related processes. For example, data collection processes established under CCAR increase regulators’ visibility into risk data, as do the FR Y-14 detailed data submissions of the top 30 U.S. banks.

A summary of the RDAR principles
- **Principle 1 – Governance**: Risk data aggregation and reporting practices should be subject to strong governance consistent with other principles and guidance established by the Basel Committee.
- **Principle 2 – Data architecture and IT infrastructure**: These should fully support risk data aggregation capabilities and risk reporting practices in normal times and during times of stress or crisis.
- **Principle 3 – Accuracy and Integrity**: A bank should be able to generate accurate and reliable risk data to meet normal and stress or crisis reporting requirements, with data aggregated on a largely automated basis to minimize errors.
- **Principle 4 – Completeness**: A bank should be able to aggregate all material risk data with data available by business line, legal entity, asset type, industry, region, and other relevant groupings.
- **Principle 5 – Timeliness**: A bank should be able to generate aggregate, timely risk data with timing depending on the nature, volatility, and criticality of the risk and on bank frequency requirements.
- **Principle 6 – Adaptability**: A bank should be able to generate aggregate risk data for a broad range of ad hoc risk reporting requests, including stress or crisis situations and supervisory queries.
- **Principle 7 – Accuracy**: Risk management reports should accurately and precisely convey aggregated risk data and reflect risk in an exact manner, and reports should be reconciled and validated.
- **Principle 8 – Comprehensiveness**: Risk management reports should cover all material risk areas, consistent with users’ requirements and the size and complexity of the bank’s operations and risks.
- **Principle 9 – Clarity and usefulness**: Risk management reports should communicate clearly and concisely, and be easy to understand yet comprehensive.
- **Principle 10 – Frequency**: The board and senior management should set the frequency of risk management reports, reflecting the needs of recipients, the nature of the reported risks, and the speed at which the risk can change (with frequency increasing in times of stress or crisis).
- **Principle 11 – Distribution**: Risk management reports should be distributed to the relevant parties, while maintaining confidentiality.
- **Principle 12 – Review**: Supervisors should periodically review and evaluate a bank’s compliance with the eleven principles above.
- **Principle 13 – Remedial actions and supervisory measures**: Supervisors should use appropriate tools and resources to require effective and timely remedial action by a bank to address deficiencies.
- **Principle 14 – Home/host cooperation**: Supervisors should cooperate with relevant supervisors in other jurisdictions regarding the principles, and the implementation of any remedial action.

Please refer to the original BCBS report for the complete, original text of the RDAR principles.²
Nonetheless, risk data capabilities of the eight U.S. G-SIBs vary. Banks that have improved their data management and reporting capabilities over the past few years will likely be better positioned to respond. Others may require a more basic analysis and face a more daunting task.

Parsing the principles
According to the BCBS document, the principles cover four topics:

• Overarching governance and infrastructure (Principles 1 – 2)
• Risk data aggregation capabilities (Principles 3 – 6)
• Risk reporting practices (Principles 7 – 11)
• Supervisory review, tools, and cooperation (Principles 12 – 14)

While broad, the RDAR principles discuss risk data expectations with unprecedented specificity. The intent of the guidance is unmistakable, however several themes require interpretation. For example, while banks are not required to express all forms of risk on a common metric or basis, risk data aggregation capabilities should be similar across systems. In addition, characteristics such as completeness, timeliness, adaptability, and accuracy have different meanings when applied to different risks, and the granularity of credit, market, and operational risk data and reports varies.

The guidance emphasizes that banks need systems capable of producing aggregated risk data for all critical risks during times of stress or crisis. Efficient risk aggregation during stress or crisis may imply a need to build in “over-capacity” relative to normal needs, including the ability to better understand “correlations” that are exhibited during crises. Aggregation capabilities should also be flexible enough to meet ad-hoc requests. This underscores the trade-off between automated capabilities (essential for timeliness and accuracy) and user defined ad hoc capabilities. The need for varying levels of granularity also implies a need for banks to consider their risk modeling infrastructure as part of their risk reporting process. This is underscored in the requirement for aggregation capabilities and risk reporting practices being fully documented and validated to a high standard, the latter potentially considering data processing and model input expectations outlined in in Federal Reserve’s Guidance on Model Risk Management Letter SR 11-7.4

Questions to consider

The RDAR principles can affect costs, timelines, resource requirements, and system configurations. To assess the implications for your organization, consider asking:

• What is the level of sophistication of our risk-related capabilities in various lines of business (LOB)?
• In our various businesses, on which of the principles are we relatively strong or weak?
• At the level of the enterprise, on which of the principles are we relatively strong or weak?
• Who inside or outside our organization might we involve in assessing these implications?

When considering implementation challenges, consider asking:

• How can our institution respond to these principles in the most efficient, yet most comprehensive manner?
• What is the gap between our current capabilities and those required to meet the new expectations?
• What should be our goals, planning horizons, and milestones for meeting the expectations and securing the intended and ancillary benefits?
• Which resources do we have—and which must we develop or access—to implement these principles?

A framework for implementation

Effective, efficient implementation of the principles likely requires coordination at three levels:

• Risk governance
• Risk management infrastructure
• Risk data management

The principles require that practices be embedded in risk governance and management processes so they permeate the risk data infrastructure, instead of one-off tactical fixes. This approach can trigger a “virtuous cycle” in which sound risk governance reinforces sound risk management, which in turn fosters sound risk data management.

3 Ibid.


From principles to practicalities Addressing Basel risk data aggregation and reporting requirements 3
1. Risk governance
Many bank boards and executive management teams have enhanced their focus on risk governance and oversight in recent years. Sound risk governance helps to ensure that the board and management understand and agree upon their risk-related responsibilities. Prominent among those responsibilities are weighing the risks of business strategies, setting risk appetite, framing risk policies, and exercising risk oversight.

Sound corporate and risk governance typically cannot occur without senior officers of the bank receiving timely, accurate information. Additionally, top-down risk appetite statements can be translated into actionable risk measurement and management practices across various risk domains through robust data management and risk aggregation capabilities. This is particularly true in the case of most banks that operate in the context of decentralized business models, which have dispersed risk management infrastructure. Standardized data management approaches and risk aggregation capabilities are foundational to risk governance and oversight.

2. Risk management infrastructure
The risk management infrastructure refers to the risk management policies, procedures, tools, and processes at the corporate and business-unit levels. The now well-accepted “three line of defense” (LOB, Risk Management, Internal Audit) approach to risk management is likely to be effective through the application of many of the RDAR principles. These functions are consumers and generators of risk data, which poses interesting conflicts in adhering to the RDAR principles. The risk management needs of businesses and functions have traditionally been defined and addressed within respective risk domains to address end-user requirements, often with little consideration to cross-functional consistency. Often a multitude of “initiatives” are launched to solve problems that end up taking a one-dimensional approach resulting in duplication, inconsistency, and control challenges. In fairness, for large complex global organizations, it is typically easier, simpler, and faster to solve problems through individual solutions that attempt to minimize or bypass dependencies to the broader infrastructure.

Figure 1. Risk governance, management processes, and systems
Having a clear understanding of the relationships across the risk management lifecycle is critically important. Figure 1 provides an illustration of the integral elements of risk management in the context of top-down aspects such as risk culture and risk appetite, and the enablement through risk data management. Both risk processes and the systems they require depend critically on an underlying data management infrastructure, illustrating the pervasive influence of data management and the need to take a holistic view to addressing any deficiencies in risk data aggregation and reporting capabilities.

3. Risk data management
Complexities in risk data management arise since risk management processes are not limited to risk management functions, but affect business units and other support functions. This should obligate business, risk management, and technology groups to have a common approach to data management. While organizations explicitly recognize these interdependencies, functional alignment and perspectives often result in impediments to operationalizing this in practice. The critical components of a data management framework are shown in the bottom half of Figure 1. Implementation of RDAR principles may be accomplished by addressing each of these components as part of a larger program.

Risk architecture and analytics
Rationalized risk data architecture is important to achieve enterprise, business unit, and legal entity reporting objectives in a consistent and controlled manner. G-SIBs, with their complex technology landscape and legacy systems, however do not always have the luxury to redefine their enterprise-wide risk data architecture. In these situations, consider approaching RDAR principles in two dimensions. At the margin, banks may find it useful to consider data quality, master data, and metadata requirements in the context of critical data elements and end user reporting requirements template for individual risk types or products (shown in Figure 1). More strategically, enterprise-wide data management framework—coupled with the risk data architecture—can embed policies, procedures, processes, and controls in data-related activities throughout the data lifecycle and data lineage such that the expectations expressed in the first eleven principles are achieved. In either case, capital investments in risk systems and tools (at corporate or LOB) must challenge any business case with alignment to the organization’s risk data architecture and strategy.

Points to consider
Viewing the RDAR expectations through the lenses of risk governance, risk management infrastructure, and risk data management helps an implementation team to coordinate needs and activities at each level. It also can provide insight into gaps and opportunities for:

• Assessing and documenting risk data infrastructure at all levels of the organization
• Identifying ways to build upon, leverage, and repurpose existing capabilities
• Employing agile development methodologies and existing integration solutions to close gaps in the risk architecture
• Taking an incremental, phased approach toward the ultimate goal of a central enterprise-wide risk data, analytics, and reporting capability
Meeting reporting requirements
Not surprisingly, external and internal reporting requirements stress an institution’s data infrastructure and controls for a variety of reasons. The graphic below (Figure 2) illustrates the problem at hand.

Individual solutions to end-to-end reporting requirements are inherently inefficient. The emphasis on capital reporting is driving a need for convergence between the risk and finance application in ways that organizations are struggling to adapt to. The BCBS principles not only require these needs to be satisfied in a consistent manner, but are also subject to adaptability and timeliness constraints. The expectations of accuracy, comprehensiveness, and timeliness are likely to necessitate common definitions and data sourcing strategy that comprehensively incorporates the various uses of data in the intermediate layers and end state. This covers the obvious items, i.e., specific regulatory schedules, but also the less than obvious such as analytics to support modeling, ad hoc portfolio analysis, management decision support, and interpretational items. An integrated approach upfront and an end-to-end view across the requirement set, while aspirational, may be the only way to (i) eliminate the “cottage industry” that has flourished in reconciling across reports and to the ledger on the back end, and (ii) ensure consistency between information needs for management reporting and external reporting.

It is part of the picture
It would likely be a mistake to view RDAR principles primarily as an information technology (IT) issue and attempt to solve the data challenges through the technology lens. While IT serves the primary role of managing systems for data sourcing and delivery, business units and risk management functions play a pivotal role in creating, modifying, and using risk data:

• Articulation of data and reporting requirements for business stakeholders (board, executive and LOB management, and regulators)
• Definition and implementation of governance and controls over data, risk calculations, and analytical processes used by risk functions and delivered in key metrics, analytics, and reports
• Alignment between risk processes and IT processes to validate and reconcile data, and controls around these processes
• Many emerging data requirements tend to be subject to interpretation and require a business perspective to establish the company’s approach

IT plays a key enabling role in supporting the business units, risk functions, management, and the board in executing their risk-related responsibilities. A partnership between LOB, risk management, and IT is likely to be essential in demonstrating progress vis-à-vis RDAR principles.
**Risk data governance and controls**

Though the terms are often used interchangeably, our framework considers risk data governance as a component of enterprise risk data management (see Figure 1). The RDAR guidelines with respect to risk data governance lay out regulatory expectations with regard to management of data quality risks, review, and approval of aggregation and reporting framework, validation standards, etc. Practically, a formal risk data governance function is necessary to achieve broader risk management objectives that extend beyond the criteria established in RDAR principles. Risk data governance should establish the scope of data management, define, and document data standards consistently across systems, and change control processes impacting risk data processes. Complementary to data governance, data management operations are affected through the four distinct disciplines described below:

- **Data quality management**: This should be considered a top-down process with data quality metrics integrated into all data streams. Data quality issues are ideally addressed in the context of the overall data governance process, preferably at the point of origination of data.

- **Master data management**: Also known as reference data, this is data used to classify and aggregate data related to transactions, positions, balances, and exposures. While errors in transactional data can lead to inaccurate risk measures, faulty master data can permeate errors systemically within the organization. Legal Entity Identifier (LEI) is an example of master data that is being embraced as a global standard.

- **Metadata management**: This is “data about the data,” and includes information about the meaning, structure, movement, change, and quality of data in various repositories. While this discipline can aspire to rationalizing the meaning of data across the company into a single, common data model, the scale of the task necessitates a gradually approach with the initial focus on few of the highest-priority data elements.

- **Data security and privacy**: Though not directly responsible for improving risk data aggregation, increases in automation and changes in regulations obligate institutions to pay increasing attention to the needs of user access, privacy, and data security.

While technology solutions do exist to address the needs of automation, the majority of the challenge within these disciplines is in rationalizing business processes to meet the needs of risk data aggregation.

**Conclusion**

Responding to the new RDAR principles is best approached in a coordinated manner. This is likely to provide the benefits of consistency and control, while minimizing data-related burdens on those who generate or use data in the course of their jobs. That said, any approach for RDAR that considers implementation or compliance through a standalone program or initiative will likely be limited in its effectiveness. Risk data infrastructure is a critical component to enablement of a variety of risk, management and regulatory reporting requirements, many of them still maturing. Hence, banks may be best served by applying and embedding RDAR principles within the existing or evolving risk management processes as well as in any new risk data and reporting initiatives.

Although this may not be easy, it is likely to be possible and worthwhile.
Contacts

Bala Balachander
Director
Deloitte & Touche LLP
+1 212 436 5340
lbalachander@deloitte.com

Vic Katyal
Principal
Deloitte & Touche LLP
+1 612 397 4772
vkatyal@deloitte.com

Dilip Krishna
Director
Deloitte & Touche LLP
+1 212 436 7939
dkrishna@deloitte.com

Tom Rollauer
Executive Director
Center for Regulatory Strategies
Deloitte & Touche LLP
+1 212 436 4802
trollauer@deloitte.com

Alok Sinha
Managing Principal
U.S. Banking and Securities Leader
Deloitte & Touche LLP
+1 415 783 5203
asinha@deloitte.com

About the Deloitte Center for Regulatory Strategies

The Deloitte Center for Regulatory Strategies provides valuable insight to help organizations in the financial services, health care, life sciences, and energy industries keep abreast of emerging regulatory and compliance requirements, regulatory implementation leading practices, and other regulatory trends. Home to a team of experienced executives, former regulators, and Deloitte professionals with extensive experience solving complex regulatory issues, the Center exists to bring relevant information and specialized perspectives to our clients through a range of media including thought leadership, research, forums, webcasts, and events.

www.deloitte.com/us/centerregulatorystrategies

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2013 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited