Beyond compliance
Gaining competitive advantage through risk data excellence
New risk data aggregation and reporting rules affect bank IT and operations

While data has been receiving more attention today in areas like cybersecurity and reporting, few senior management teams consider data a critical and strategic agenda topic. Given the urgency of competing economic and regulatory demands, data management policies and practices are often assigned low priority. Yet this oversight represents a hidden danger. Simply stated, management reliance on incomplete, inaccurate or stale data can compromise business decision-making.

The issue is exacerbated by the fact that data, from capture through to aggregation processes, is often not fit for purpose. Many financial institutions must engage in extensive data cleansing and manual reconciliation before they can produce reasonable aggregated, and often basic, management reports. To complicate matters, the work effort required to cleanse, manipulate and reconcile data often prevents analysts from fully understanding key metrics and their associated business implications.

In an effort to address this issue, the Basel Committee on Banking Supervision (BCBS) issued 14 principles aimed at strengthening risk data aggregation and risk reporting. While ostensibly focused on risk data, the principles are ultimately about enabling banks to make timely, consistent and informed decisions.

Given the current state of affairs at most banks, compliance with these principles will result in significant impacts on operations. Global systemically important banks (G-SIBs) must comply with these principles by January 2016, and are expected to undertake annual self-assessments and produce remediation and implementation plans to address any gaps. In Canada, the Office of the Superintendent of Financial Institutions (OSFI) expects domestic-SIBs (D-SIBs) to comply by December 2016. Both BCBS and OSFI have set expectations that any bank newly designated as G-SIB or D-SIB must comply within three years of the designation. Over time, these principles will likely be further rolled out and represent the minimum data quality and governance standards that apply to all regulated banks and insurers.

---

1 Basel Committee on Banking Supervision, “Principles for effective risk data aggregation and risk reporting” (BCBS 239)
Inside the BCBS principles

According to the BCBS Principles for effective risk data aggregation and risk reporting, the 14 principles address four key themes:

<table>
<thead>
<tr>
<th>Key theme</th>
<th>BCBS principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance and infrastructure</td>
<td>1. Governance</td>
</tr>
<tr>
<td></td>
<td>2. Data architecture and IT infrastructure</td>
</tr>
<tr>
<td>Risk data aggregation capabilities</td>
<td>3. Accuracy and integrity</td>
</tr>
<tr>
<td></td>
<td>4. Completeness</td>
</tr>
<tr>
<td></td>
<td>5. Timeliness</td>
</tr>
<tr>
<td></td>
<td>6. Adaptability</td>
</tr>
<tr>
<td>Risk reporting</td>
<td>7. Accuracy</td>
</tr>
<tr>
<td></td>
<td>8. Comprehensiveness</td>
</tr>
<tr>
<td></td>
<td>9. Clarity and usefulness</td>
</tr>
<tr>
<td></td>
<td>10. Frequency</td>
</tr>
<tr>
<td></td>
<td>11. Distribution</td>
</tr>
<tr>
<td>Supervisory expectations</td>
<td>12. Supervisory review</td>
</tr>
<tr>
<td></td>
<td>13. Remedial actions and supervisory measures</td>
</tr>
<tr>
<td></td>
<td>14. Home/host cooperation</td>
</tr>
</tbody>
</table>

The BCBS risk data aggregation and risk reporting (RDAR) principles set unprecedented expectations that are open to individual banks for interpretation. For example, while banks are expected to possess common risk data aggregation capabilities across their systems, there is no singular metric required to express different forms of risk. Similarly, characteristics such as completeness, timeliness, adaptability and accuracy can have different meanings when applied to different risks.

The granularity of credit, market, operational and liquidity risk data and reports also varies. In fact, this need for varying levels of granularity may require banks to take their risk modeling infrastructure into account when developing their risk reporting process. Unless banks enhance their risk data aggregation infrastructure, they will be unable to properly meet requirements to fully document and validate the strength of their risk aggregation and reporting capabilities.
Similar challenges exist for banks when dealing with aggregated risk data for 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. At the same time, aggregation capabilities must remain flexible to meet ad hoc requests. As a result, banks must find a balance between the use of automated capabilities, which are essential for timeliness and accuracy, and reliance on manual ad hoc processes.

The reliance on manual processes and the significant shortcomings of the IT infrastructure were reflected in the initial G-SIB self-assessments completed. Data architecture and IT infrastructure compliance scored lowest of all principles, while risk report distribution scored highest. Since governance and IT infrastructure principles are “preconditions to ensure compliance with the other principles”, this raises questions regarding the value and reliability of the risk reports if the systems to produce them have limitations.

Banks must carefully analyze and factor all of these implications and preconditions into their implementation plans.

**Beyond box-checking**

Given the ambiguous nature of the BCBS principles, it can be tempting for banks to adopt only minimal compliance standards when developing risk data aggregation and reporting principles. However, this minimalist approach is likely a mistake. When viewed through an enterprise lens, the initiatives prescribed by the RDAR principles create an opportunity to unlock the strategic power of a bank’s data. By enhancing your risk data policies, standardizing your processes and embracing automation, you can:

- **Improve** decision-making by enhancing data integrity
- **Create** new insights to support enterprise-wide decision-making rather than taking a siloed approach
- **Update** enterprise data (e.g. finance and treasury data) with relative ease
- **Free up** risk managers to perform analytics rather than data processing and consolidation

---

2 Basel Committee on Banking Supervision, “Progress in adopting the principles for effective risk data aggregation and risk reporting” (BCBS 268)
Without this strategic lens, the changes required for the RDAR principles will be viewed as just a regulatory cost and likely not be adopted in practice. This concept was likely similarly noted by BCBS, who in their progress report suggested that supervisory authorities “consider enhancing their efforts to fully integrate the Principles into their supervisory programs”\(^1\). With the strategic lens, the changes can help meet regulatory compliance needs and transform data into a strategic asset. The key is to get senior executive buy-in, develop a plan that takes an enterprise view to compliance and build a strong foundation that lays the groundwork for enterprise data transformation. Let’s look at each of these elements in turn.

**1. Getting executives to recognize data as a strategic asset**
Because risk data is sourced and transformed in various areas throughout the bank and not solely within risk management, it is particularly complex to manage. That’s why enterprise-wide management buy-in is essential before banks can effectively make the changes required to comply with the RDAR principles. As RDAR program decisions and changes find their way to the front line, management from both the business and technology teams must champion the true value of risk data. With this early buy-in, banks will be much better positioned to develop RDAR implementation plans that are effective and executable, not only within risk management, but across the organization.

**2. Taking an enterprise view by planning for strategic value rather than minimal compliance**
Building a RDAR compliance and implementation plan is a broad and deep initiative. To fully unlock the strategic value of your data, it makes sense to initially launch the plan for risk data and then subsequently roll it out across other data types. Too often, large banks undertake significant initiatives in a silo with no consideration to their potential application in other areas of the organization. This can lead to unwarranted duplication of both time and money. To avoid this outcome, banks should approach RDAR implementation strategically by interpreting the RDAR principles broadly enough to apply to all forms of data, not just risk data. By taking an enterprise view, you can go beyond mere compliance to unlock the full value of your data across the organization.

**3. Building a foundation that solves once for risk data and applies across the enterprise**
Solving once also requires you to adopt tools and accelerators at the enterprise level. In this way, the foundation of the RDAR program can apply as much to risk data as to finance data or customer data. In essence, risk data can be viewed as the pilot program of a much larger and more valuable initiative to optimize data across the bank. Where possible, seek opportunities to leverage existing practices and tools, particularly where you have already gained user buy-in and learned key lessons.

---

\(^1\) Basel Committee on Banking Supervision, “Progress in adopting the principles for effective risk data aggregation and risk reporting” (BCBS 268)
After considerable analysis, the BCBS found that current data aggregation and reporting activities at many financial institutions present a staggering variety and number of areas where data can be degraded, corrupted, lost or misdirected. These gaps negatively affect the quality and timeliness of business decision-making. Fortunately, the BCBS RDAR principles provide a framework banks can use to solve this problem at its source. To do so effectively, however, banks must understand the futility of implementing the new RDAR principles in a decentralized manner, as such an approach fails to provide the necessary context to translate the principles into business and risk management activities. In contrast, a centralized approach provides the benefits of consistency and control, while minimizing data-related burdens on those who generate or use data in the course of their jobs.

Adopting this type of centralized approach requires a commitment of both leadership and investment. The following four steps can help streamline implementation:

- **Start** at the top by identifying the organization’s information requirements and defining its risk appetite, key metrics and reports required (and desired) by the board and senior executives.
- **Translate** those definitions to meet the operational and reporting needs of risk functions and business units, for example, for risk tolerances, credit and trading limits.
- **Convert** these needs into implementation milestones within a data management framework.
- **Address** any identified data management gaps by using a combination of business process changes and technology. This may require changes in risk data architecture.

No matter how you approach implementation, it is critical to avoid viewing the task solely as an exercise in regulatory compliance. The RDAR principles, when embedded across the organization, should lead to superior data capabilities that yield benefits beyond risk reporting. Ideally, this results in one well-managed, central, reliable data source, which reconciles to the general ledger and adds value to the business. From a business perspective, banks can minimize or eliminate redundancy across business silos, realize cost savings and benefit from a flexible, scalable platform and vastly improved risk governance and risk management.
Contact us
For more information about the BCBS principles and the benefits of an enterprise-wide RDAR implementation, contact:

Azer Hann
Partner
Risk and Capital Management Lead
416-601-5777
ahann@deloitte.ca

Gord Kilarski
Director
Risk Analytics Lead
416-601-5677
gkilarski@deloitte.ca