Basel and Beyond: Transforming Regulatory Burden into Business Opportunity
Introduction

The risk reporting requirements for banks have taken a deliberate turn towards being more detailed and prescriptive. Banks are struggling on one hand to understand and catalogue the requirements coming from a mushrooming set of regulators, and on the other hand scrambling to get their data house in order to ensure compliance. It is a challenge that requires significant resources and planning to meet.

A hierarchy, an order, is emerging to help banks structure their thinking and their response. Whether an institution is global or limited to a single jurisdiction, whether diversified or single product line, there are emerging best practices to help tackle the relevant regulatory risk challenges.

This white paper will bring forth the evolution of the regulatory risk reporting environment, detail specific critical elements of the primary regulatory rules, and propose a framework for ensuring a readiness in data management capabilities that drives compliance. It provides guidelines to help financial institutions navigate the complexities of regulatory requirements and to transform regulatory burdens into business opportunities. It explores the key regulatory requirements that could impact risk data governance, aggregation and reporting for financial institutions operating both globally and in the United States. It will also look at how these “regulatory burdens” on risk data may also open significant business opportunities to streamline global operations and enhance risk management systems.
The Rise of Regulators Providing “Data Guidance”

The recently released annual report from the US Office of Financial Research (OFR) spent nearly as many pages explaining the importance of reference data, data gaps, and related esoteric terms of “taxonomies” and “ontologies” as it did on the actual reporting of the systemic risks to the financial system.¹ Established by Dodd-Frank and operating under the auspices of the Treasury, the OFR not only is tasked with studying and reporting on the risks to financial stability, it also is mandated to understand risk data gaps in order to standardize that data across financial institutions feeding into their risk analysis.

In fact, the OFR is not alone in its mandate to improve the quality and scope of risk management. The field is actually somewhat crowded, and the OFR to date has not taken as prominent a role when compared to the Basel Committee on Banking Supervision (BCBS), which published its 239th publication, Principles for Effective Risk Data Aggregation and Risk Reporting, or even the potential impact of the US Federal Reserve’s Enhanced Prudential Standards (EPS). Oddly, the global goal to standardize and unify risk data governance, aggregation, and reporting has produced a proliferation of the number of organizations playing a role in achieving it. There are not only the OFR in the United States and the traditional regulators like the SEC, CFTC, OCC, and the Federal Reserve, but also global bodies, such as the BCBS and the FSB, and regional bodies, such as ESMA, ECB, and ESRB. Clearly no organization is “unique” in setting the standards to which financial institutions must adhere if they are to avoid the pitfalls of noncompliance.

The Coming of Age of Governance, IT, and Analytics

Risks (including market, credit, liquidity, operational) and the underlying data (from seemingly mundane reference data to ratios and assets) are no longer relegated to traditionally siloed functional areas such as regulatory reporting, financial reporting, or internal business KPIs. Capabilities in this area have been elevated to the board level. It would have been difficult to predict that today’s boardrooms would be buzzing with discussions about “critical” data and metadata strategies.

Boards and top management have busted through traditional barriers to enterprise information management, such as cost considerations, and are relentlessly pursuing the goal of achieving enterprise-wide risk data governance, aggregation, and reporting. The force driving this change is the sting associated with the substantial rise in regulatory fines. For 2014, and for each of the past few years, global regulatory fines reach new levels and now stand to the tune of 56 billion dollars, according to the Financial Times.² This excludes the significant set asides and legal cost that have been impacting the bottom line of banks.

Additionally, the evolving capabilities associated with big data, master data management, and analytics broadly support the build-out of new risk data aggregation and reporting. “With an increased focus on front-to-back processing, an expansion in the breadth and depth of risk metrics, and the growing complexity of banks’ global regulatory environment,” the US Federal Reserve’s Advisory Committee highlighted early in 2014, a key new technological enabler is “Big Data and the corresponding analytics.”

### The Focus of Sweeping Regulatory Requirements on Data Readiness

There are several key regulatory requirements that are consuming the attention and resources at financial institutions and that have significant implications in the areas of risk data governance, aggregation, and reporting. The following rules are significant both in their near-term requirements and sweeping in terms of the required data readiness.

#### BCBS 239

The BCBS release in 2013 on risk data governance, aggregation, and reporting principles is the global de facto benchmark and requiring the highest principles to attain. It is significant in its detailed requirements that are categorized under three headers and eleven core principles, with the expectation that all of the principles are met simultaneously and not at the expense of each other. The three headers cover:

1. **Overarching Governance and Infrastructure.** Implement a strong governance framework, combined with a risk data architecture and IT infrastructure, led by the board with senior management ownership to support aggregation and reporting principles.

2. **Risk Reporting Practices.** Provide accurate, complete and timely data to the right decision makers, in the right time frame, and reflecting the appropriate information.

3. **Risk Data Aggregation Capabilities.** Develop and maintain strong risk data aggregation capabilities to ensure the reporting reliably reflects risks regardless of legal entities and jurisdictions.

While BCBS 239 details the framework and processes surrounding risk data governance, aggregation, and reporting across an entire financial institution, there are at least three key additional documents released by BCBS that may have significant impact on implementation. These include *Basel III: A Global Regulatory Framework* revised in June 2011, for intraday liquidity requirements (BCBS 248), *Monitoring Tools for Intraday Liquidity Management*, and the earlier 2008 release of *Principles for Sound Liquidity Risk Management and Supervision*.

The implementation date for BCBS 239 is by the start of 2016, with particular focus on those named as global Systemically Important Banks (G-SIBs). Recent reports show that many firms will have difficulty meeting this deadline, and the penalties that may ensue are unclear. As BCBS does not have an enforcement arm, the primary regulator of each country is expected to ensure compliance.

---

ENHANCED PRUDENTIAL STANDARDS (EPS)
A significant development for the largest banks has been the US Federal Reserve’s Enhanced Prudential Standards (EPS) that came out in early 2014 and are effective January 2015. Firms can view EPS as one means for the US Federal Reserve to align with BCBS 239. This latest update to the rules should also be read in conjunction with the 2012 release of the Fed’s SR Letter, Supervision Framework of Large Financial Institutions. Additionally, banks that fall under the OCC also need to comply with Heightened Standards, released late 2014, extensive guidelines covering risk data governance, aggregation, and reporting. For the largest foreign banks (FBOs), there are further considerations and are considered separately below.

For all larger banks (above the $50 billion threshold), the rules set specific risk management frameworks and requirements, including the establishment of a risk committee and of the governance, procedures, and risk control infrastructure. The scale and scope of the expectations are dependent on the size of bank. Those designated under the Large Institution Supervision Coordinating Committee (LISCC), the combination of relevant G-SIBs and G-SIIs (the insurance counterpart) plus one (GE Capital), have the highest expectations of a risk management framework.

Banks that are not sized for “full” EPS (less than the $50 billion threshold but more than $10 billion) have key requirements and responsibilities that impact risk data governance, aggregation, and reporting by July 2015. This includes the mandate for a globally responsible risk committee with management governance, procedures, and controls, as well as additional requirements related to identifying and reporting risk management gaps.

CCAR
Now into its fifth year (latest results announced in March), the Fed’s Comprehensive Capital Analysis and Review and other related stress testing (e.g., DFAST) came about from a mandate under Dodd-Frank. Under CCAR, the implementation of risk data governance, aggregation, and reporting framework will be effectively tested and monitored. Firms can view this as one possible mechanism to “test” for compliance with sections of BCBS 239.

The Fed’s annual submission process is both a qualitative and quantitative assessment of essentially the entire risk environment of a bank. The qualitative process, as defined by CCAR, is the Fed’s determination of the robustness of the corporate governance processes and controls that support CCAR.

FBOs and Intermediate Holding Companies (IHC)
For FBOs in the US at the $50 billion threshold, the impact of EPS has been added a significant structural re-organization requirement as mandated by the new EPS rules. These requirements, which could affect about seventeen foreign banks in the United States, must be accomplished in parallel to implementing BCBS 239 and EPS (although CCAR 2015 has made a “one-time” concession to ongoing changes to fulfill the requirement).
Boards and top management are relentlessly pursuing the goal of achieving enterprise-wide risk data governance, aggregation, and reporting.
While there is much detail in the new structure, a US-based risk officer and risk committee is mandated for covered FBOs, impacting the build-out of a governance and risk management framework. In addition to impacting risk data aggregation and reporting, the potential complex reorganization could create significant uncertainty in any large-scale implementation of reference data and other IT systems. The new IHC structure is required by July 2016.

**Dodd-Frank (Swap-Dealer/Major Swap Participant and Volcker Rule)**

For financial institutions that operate and register as a Swap-Dealer (SD) or Major Swap Participant (MSP), many of the details, especially from the CFTC-side, have been released over the past few years. However, there are ongoing developments, especially technical data standards, which may impact risk data aggregation and reporting.

More recently, the SEC released the set of rules for the transparency of the security-based swap market, including those relating to security-based swap data reporting and public dissemination (SBSR). This recognizes, for example, the need for the Swap Data Repositories (SDRs) to utilize a key risk data standardized attribute, the Global Legal Entity Identifier System (GLEIS). The expected compliance date may be early 2016. (Note: This is pending publication.)

While there has been much discussion around the recent further delay and potential repeal of the Volcker Rule (section 619), aspects of the Rule are already implemented (Appendix A) when relevant to a bank’s business, especially for those reporting with large trading activity. Risk metric reporting, recently implemented for large-sized operations (greater than $50 billion in trading assets/liabilities), will, for medium-sized operations (less than $50 billion but greater than $25 billion), become effective May 2016. The Rule also imposes scaled levels of standards of risk governance programs and outlined in detail in Appendix B of the rule, with the current conformance date set for July 2015 (for relevant operations).

**ECB SSM**

The much anticipated and recently launched (in late 2014) European Central Bank’s Single Supervisory Mechanism is a potentially major new player in writing the standards and requirements covering risk data governance, aggregation, and reporting.

With oversight of over nearly five thousand financial institutions in Europe and the mandate to ensure common standards and methodologies, the SSM has established the Supervisory Policies Division to develop the prudential requirements in the risk space. The rule is not yet released, and no estimate of the date is firm at this time.

---

CRD-IV/CRR
The European Capital Requirements Directive and the Capital Requirements Regulation, issued by the European Union government, are a crucial component to the build-out of risk data governance, aggregation and reporting as it relates to the core of the implementation of Basel III in Europe.

While applicable beginning in 2014, it is an evolutorial process and essentially parallels the full Basel III implementation process through the EBA and national regulators, currently set to end in 2019. In addition to driving the goal of standardizing European reporting, such as FINROP and COREP, it also takes on risk governance. As the release highlighted, the directive’s intent is to overcome “inadequate group wide risk management and insufficient governance.” This requires significant data modeling and scenario development.

The most recent updates by the EBA include consultations amending implementing technical standards (ITS) for Liquidity Coverage Ratio (LCR) and Leveraged Ratio (LR) and final draft Regulatory Technical Standards (RTS) on Countercyclical Capital Buffer (CCB).

MARKETS IN FINANCIAL INSTRUMENTS DIRECTIVE II (MIFID II)
In addition to the large-scale implementation of CRD-IV, MiFID II (and the related regulation MiFIR), slated for 2017, is a crucial component to incorporate in any planning for risk data reporting.

ESMA, the body leading the charge, recently released a consultation of over 600 pages outlining extensive regulatory technical and implementing standards (RTS/ITS) covering all aspects of risk-related data for financial instruments. In the consultation, ESMA does acknowledge some challenges the consultation may pose, appreciating that it “will be difficult” standardizing some types of reference data. On the broader governance function, the current consultation generally upholds previous guidance.

UCITS V (ASSET MANAGEMENT)
UCITS V, known as Undertakings for Collective Investment in Transferable Securities (and the similar requirements for alternative investments, AIFMD), was officially adopted in late 2014 after many years in discussion and will be effective March 2016. The latest UCITS version is relatively limited in terms of risk data governance, aggregation, and reporting, but ESMA is tasked during 2015 to identify and develop detailed practical requirements. The Risk Management Principles for UCITS remains as published by ESMA in 2009 and generally addresses governance in broader terms than BCBS 239.

In general, asset managers have not been the focus of attention in this space and for some in the industry the “bank-centric” nature of many of the requirements should not be imposed. Only one asset manager, State Street, is currently on the G-SIB list. This lack of attention may be changing, as SEC Chairperson Mary Jo White highlighted in a speech in December when

---

discussing the enhanced standards needed for the asset management industry: “We must improve the data and other information we use to draw conclusions about the risks” in the industry.8

**Five Essential Steps to Risk Data Readiness**

Given the detailed and stringent requirements, firms cannot adopt an ad-hoc approach to compliance with regulatory risk rules. A holistic, enterprise-wide effort to get the “data house in order” is the best practice. Based on extensive experience building these capabilities, here are the five key components of a data strategy built for the realities of today’s regulatory landscape:

1. **Build a centralized data governance process and organization.**

   Data Governance is not just about data. It is also about the business processes, decisions, and stakeholder interactions that an organization needs to enable. Therefore, it is more appropriate to consider Data Governance as the holistic management of the availability, usability, integrity, and security of information employed in an enterprise to enable business outcomes.

   Best practices for an effective Data Governance program include having a governing body, a defined set of policies and procedures to guide decisions aimed at achieving desired outcomes, and a plan to execute those policies and procedures in an operational capacity.

   The operational aspects of Data Governance program are implemented via what is known as a Data Governance operating model. The operating model defines the organizational structure (most always cross-functional and matrixed), roles, and responsibilities to execute all of the tasks and processes required to achieve the desired outcomes set out by the program.

2. **Understand the necessary data usage needs.**

   Firms often fail in their Enterprise Information Management efforts because their data strategies fall short in one critical area: the consumption model. Many “successful” data strategy implementations satisfy technical requirements and fail user requirements. That will not work when establishing risk data preparedness.

   Regulatory imperatives demand that data not only be accessible, but that it be presented in specific formats within defined time constraints. This means a new level of capability in for enterprise data mining, alerts, dashboards, and reporting.

3. **Establish a data management operating model.**

   Preparing an organization’s data for regulatory risk compliance requires the establishment of an organization with defined roles, responsibilities, and processes. The data management function is the guts of the capability needed to deliver on the varied requirements.

A holistic, enterprise-wide effort to get the “data house in order” is the best practice.
In order to set up the right organization, key service categories must be defined and staffed, and processes must be implemented. The services central to data management include planning and demand management, build and test, release to production, change management, and others. This is where the movement of data, the warehousing of data, and the accuracy of data are all managed.


Data Quality Management (DQM) is a program which underpins the operational aspects of a Data Governance program. It involves defining business rules for ensuring the efficacy of data, a process to remediate Data Quality issues, and corresponding set of metrics that can be reported on to measure and monitor data quality over time. Data Quality can be thought of in the following dimensions: Completeness, Uniqueness, Validity, Accuracy, Integrity, Timeliness, Consistency, and Representation.

It is important to lay out a complete DQM future-state vision, but to start small. Do not attempt to “boil the ocean” with your DQM program by trying to implement it all at once. A solid implementation roadmap that starts small and builds the program up over time is the best approach.

Establishing DQM is not a one-time event, but rather an ongoing process that will evolve over time. Effective DQM is often a cultural shift in an organization and takes time. The DQM program should be re-evaluated periodically and modified as required.

The table below highlights the intersection of these dimensions with the principles of BCBS 239:

<table>
<thead>
<tr>
<th>BCBS 239 Principles</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance &amp; Infrastructure</td>
<td>Design, build, and maintain data architecture and IT infrastructure for normal times and stress events</td>
</tr>
<tr>
<td>Data Architecture &amp; IT Infrastructure</td>
<td>Design governance framework with Board oversight of implementation of the principles</td>
</tr>
<tr>
<td>Accuracy &amp; Integrity</td>
<td>All material risk data captured and aggregated</td>
</tr>
<tr>
<td>Completeness</td>
<td>Aggregated and up-to-date risk data available in a timely manner and maintaining principles</td>
</tr>
<tr>
<td>Timeliness</td>
<td>Need to meet broad demand of user requests and changing requirements in normal and stressful situations</td>
</tr>
<tr>
<td>Adaptability</td>
<td>Accurate and precise aggregated data reflecting risk in exact manner for the Board and senior management</td>
</tr>
<tr>
<td>Accuracy</td>
<td>All material risk areas captured; depth and scope appropriate to risk profile</td>
</tr>
<tr>
<td>Comprehensiveness</td>
<td>Communicate information in clear and concise manner and easily understandable to inform decision-making</td>
</tr>
<tr>
<td>Clarity &amp; Usefulness</td>
<td>Board and senior management set frequency based on needs of recipient and the importance to sound risk management</td>
</tr>
<tr>
<td>Frequency</td>
<td>Reports distributed to relevant parties while maintaining confidentiality</td>
</tr>
</tbody>
</table>

Table: BCBS 239 Principles across Enterprise Information Management Framework Capabilities
5. Invest in architecture to build a solid data house.

Proper data architecture is not just a good idea. It is an explicit, detailed regulatory requirement. The principles that guide proper data architecture are:

a. Information must be relevant to the business and customers. Data management and modeling should standardize information definitions, providing a centralized control point for the architecture and establishing a common vocabulary for information.

b. Information must be timely, providing the business and its customers with information when they need it. Using the reference data architecture framework as a control point, an organization will be able to map existing and new data as it is on-boarded to common definitions and mappings, ultimately establishing a semantic-based architecture.

c. Information must be trustworthy, exceeding expectations for consistency, completeness, and accuracy. Introducing concepts of Master Data Management will enable standardization and develop trust for all critical identifiers for the information entities that are most crucial to running the business.

**Unintended Consequence: A New Era of Analytic Capability**

It is clear that firms face a steep climb to summit the regulatory risk mountain. What is also becoming clear is that firms can realize tremendous business value by leveraging these newfound capabilities. The improvement in data quality, availability, and transparency required by ever-increasing regulatory requirements will unlock unprecedented advancements in understanding customers, employees, and operations.

Knowledgent envisions a “golden age of analytics” that will usher in business transformation in three critical areas, above and beyond those addressing compliance:

1. Customer-centricity efforts. The vision of building a one-to-one relationship with all customers on their terms does not work with “cookie-cutter” approaches to customer experience. Next-generation data access and quality will enable the kind of experience that drives customer acquisition, retention, and satisfaction.

2. Sales effectiveness. Elevating the discussion with customers is an imperative felt from the highest-touch relationship manager to the call center. Integrating and correlating the information firms have about their customers and arming customer-facing representatives with insights and ideas will change the game and affect market share.

3. Operational effectiveness. Just as important as “knowing your customer” is “knowing your business.” Fact-based decision making is a best practice in management. New insights based on access to integrated, reliable data will drive strategy and operations to higher levels of precision and effectiveness.

The burdens of compliance with regulatory requirements, such as those noted in BCBS 239, can take their toll on financial institutions already grappling with the challenges presented by ever-increasing amounts of data. However, these burdens also present an opportunity to deliver better data management and governance, reduced risk, and high-value business impact.
Additional Resources


ABOUT KNOWLEDGENT

Knowledgent is a data and analytics firm that helps organizations transform their information into business results through data and analytics innovation. Our expertise seamlessly integrates industry experience, data analytics and science capabilities, and data architecture and engineering skills to uncover actionable insights.

Knowledgent operates in the emerging world of big data as well as in the established disciplines of analytics and visualization, strategy and engineering, and governance and operations. We have not only the technical knowledge to deliver game-changing solutions at all phases of development, but also the business acumen to evolve data initiatives from ideation to operationalization, ensuring that organizations realize the full value of their information.

For more information about Knowledgent, please visit www.knowledgent.com.