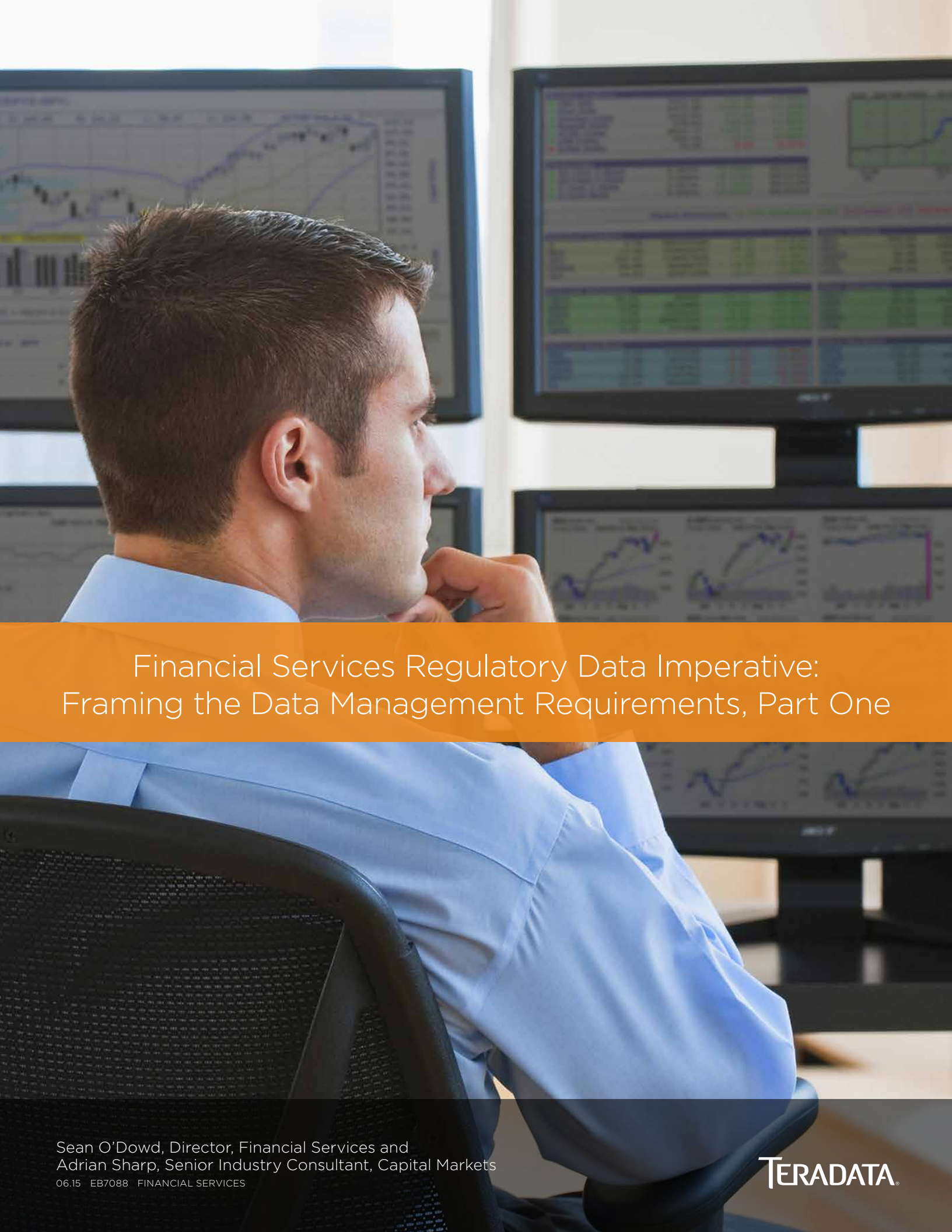

Financial Services Regulatory Data Imperative: Framing the Data Management Requirements, Part One

Sean O'Dowd, Director, Financial Services and
Adrian Sharp, Senior Industry Consultant, Capital Markets

06.15 EB7088 FINANCIAL SERVICES

TERADATA.

Table of Contents

Introduction

Addressing the financial, risk and compliance requirements within a financial services organization is now dependent upon a firm's ability to master the lifecycles of its data structures in a highly transparent manner. This paper defines current internal and external regulatory data requirements based upon the impact of "The Great Recession", as well as tactics to address compliance while retaining shareholder value and optimizing internal and consultative resources.

Executive Summary

Optimizing product offerings and pricing were once the financial services industry's top priorities. However, in the wake of the 2008 financial crisis, heightened regulatory scrutiny has forced organizations to more transparently connect their knowledge assets for the purposes of risk management, financial analysis, and financial instrument lineage.

Leveraging the knowledge gained from the post mortem of the "Great Recession" and efforts such as the BIS Quantitative Impact Studies (QIS), regulators are now examining and evaluating data storage and handling practices, analytic processes, and business execution—and the governance over all three. Of increasing importance is the concept of end-to-end validation of business processes. Key questions, such as "How do you govern and validate your business processes?" are emerging during exams and oversight meetings. And complete transparency of data lifecycles is critical to demonstrate compliance.

In response to increased scrutiny, institutions are now faced with large investments in internal audit and process oversight departments, as well as external consultancies. Here, data provenance, or lineage and pedigree, which describes the source (origin), derivation, history and context of data, is key to exhibit to auditors that a firm is proficient in its risk and capital processes. A company's ability to systemically connect data quality, data scrubbing processes, data extraction, transfer and load processes, and manual interventions is an examination topic for both internal auditors and external regulators (domestic and international).

The more efficient a company's compliance processes are, the less constrained it will be by regulatory criticism, which often leads to undesired reputational risk. Resources and potential funding once allocated to addressing those regulatory criticisms can now be earmarked for innovation efforts in customer products and services. Gaining additional usage from compliance data management investments across the business could be considered a "regulatory dividend".

Compliance is also a key driver of shareholder value. An organization's ability to connect their data through the life cycles of their customers and products—while simultaneously leveraging that data to acquire and manage relationships—will determine which organizations will succeed and which will face continued heightened regulatory and investor challenges.

In addition to increased external scrutiny, institutions are now faced with large investments in internal audit and process oversight departments.

Post 2008: New Regulatory Expectations

Background

In reaction to the financial crisis of 2008, state and federal regulatory agencies—and regulations—expanded. Institutions now need to address two types of regulations: traditional, external regulation from federal and state agencies (Basel or Dodd Frank); and internal regulation (i.e. internal audits, program management, and process challenge teams).

Impact and Tactics to Consider

With stability no longer a guarantee, companies must grow their internal regulatory practices to demonstrate adherence and value to investors and shareholders. Institutions have made massive investments to create teams of internal or consultant auditors and program managers to help define and manage all identified risk gaps. The theory behind the concept of self-regulation is this: Layer more process oversight into organizations so issues that pose risks to the business won't fall through the cracks. In other words, teams must examine every potential financial and operational risk, document each one, and demonstrate remediation strategies.

A firm's financial and operational process data has also become increasingly important. An organization may have a low-risk profile, excellent internal controls, and superior process management strategies. However, without an effective data model, it will fail to execute its regulatory mandate.

An organization may have a low-risk profile, excellent internal controls, and superior process management strategies. However, without an effective data model, it will fail to execute its regulatory mandate.

Data Models and Analytics

Background

In addition to the traditional safety and soundness exams for lending and financial processes, regulatory exams now focus on data models and analytics practices as core concerns.

The data component covers a host of issues on the governance and quality of data. Financial institutions large and small have to demonstrate what their data models are, how data elements are defined, how the flow of data is controlled, how data is managed and used. From this point in time, Executive Managers should expect data quality to be a component of every regulatory interaction going forward.

Impact and Tactics to Consider

In response to increased external scrutiny of data models and analytic practices, financial institutions are making dramatic changes in both the scope and design of their internal governance processes. Organizations expand their audit teams to include specialized audit groups that conduct internal reviews of data sources, structures, controls, and the documentation on the flow of information throughout the enterprise.

As a whole, the financial services industry is in the process of internally remediating thousands of internal audit findings on failed data definition, transport, and oversight controls. Oversight becomes a cascading consequence for many organizations because, as the internal scrutiny of audit teams increases, specialized data quality teams are being created.

To cope with the shifting landscape of data oversight, many organizations take painful steps to address their data definition, acquisition, storage, access and transport strategies. The quality of the organization's data model is no longer the domain of the technology teams, but is now both a risk and a line-of-business imperative. Internal audit teams are being re-tooled to follow the end-to-end flow of data from an external market vendor to its practical business group use. Any gap or failed control that's found along the way is likely to be identified and called out in an audit.

Data quality issues and concerns have prompted mandates for institutions to demonstrate and prove their data models like never before.

Executive managers need to examine investment in improved data models. Or, they must consider investment in ongoing change requirements to fix broken data models. While the cost of addressing a new data model is significant, the cost of changing a broken data model is enormous.

Institutions also deploy another form of internal regulation known as program management organizations (i.e., PMOs). Longtime fixtures in the manufacturing industry, PMOs are now commonplace within financial services. Internal oversight is a risk mitigation effort that helps ensure major gaps in financial and risk management processes do not form (and to address them systematically if they do). The role of PMOs is to put structure on internal financial, risk and technology teams and to oversee how requirements are formed and execution is tracked. In addition to external regulators, internal auditors' business lines are now deeply integrated with program management processes. The reduction in execution volatility has become increasingly important to financial institutions, and the investment in people tasked with overseeing execution reduces both volatility and risk to the enterprise.

The role of data, including its structure, definition and flow, is critical to an organization's compliance profile. Data systems need to define and measure data quality in ways that provide real-time intelligence to regulators and operational risk managers. One example of this concept is a data warehouse that imports trading or loan decision data. It is no longer acceptable for that data to simply move efficiently. It now needs to be measured in-flight for both content and volatility in a way that's completely transparent to auditors and process managers.

Data structures need to function to meet the needs of both end users and oversight entities.

Data Lineage: The End-to-End Imperative

Background

The introduction of BCBS 239[1] (Basel Committee on Banking Supervision) in 2013 formalized the requirement to prove data lineage across the data lifecycle in risk data aggregation and reporting. A recent research report from Lepus[2] asked banks about their ability to meet the requirements. The vast majority (89%) stated that they require improvements to be made in this space, with 22% stating that significant investments are required. While there is a general lack of understanding in the industry, proving data lineage is now unavoidable, especially given the January 2016 deadline for BCBS239 compliance.

> The aggregation of data from its basic form through attribution into business intelligence is what drives business processes.

Impact and Tactics to Consider

The requirement for end-to-end, data management has caused financial services firms to invest heavily in defining business models, rationalizing data processes, and documenting data controls and transformations throughout all data use life cycles. Many banks, investments firms, and insurance companies have found that at the end of the sometimes painful clean-up of data processes and the rationalization of data models, businesses run more smoothly and achieve stronger financial results.[3]

When data moves through an organization, it transforms from a raw state to a refined business use. For example, consider the purchase and input of a raw risk attribute. The attribute is a single point of information on a contract. That attribute is then either used as a simple descriptor or segmentation lever, or it's combined with another attribute and subjected to a mathematical formula. These uses and transformations occur millions of times each day. The aggregation of data from its basic form through attribution into business intelligence is what drives business processes. The ability of an enterprise data management and governance system (in general) to encompass the capabilities of defining data elements, tracking their transformations, and measuring volatility is an absolute imperative in the new regulatory environment.

The 2008 financial crisis brought the qualitative aspects of risk management under regulatory scrutiny, including specific expectations for Risk IT and risk data culminating in BCBS 239. Many IT practitioners consider that demonstrating technical lineage (the equivalent of systems and data-flow diagrams) is sufficient. For risk professionals and regulators, however, this is entirely too general. Proving data lineage is the digital equivalent of an accounting audit and should be approached with the same degree of rigor and discipline.

EAI (Enterprise application integration) and metadata management tools are frequently touted in response to meeting the data lineage challenge. The reality for most G-SIBs (Global systemically important banks) and their domestic counterparts, D-SIB (Domestic systemically important banks) is an array of different technologies and data silos, which employ multiple third party and home grown EAI and ETL (extract, transform and load) integration and aggregation components.

Metadata (or 'data about data') includes a broad array of business and technical elements. Proving lineage requires that these metadata elements are captured for each change of state and each data instance. Before these technologies can meet the regulatory requirement, there have to be mechanisms to "stitch" these elements together in a repeatable manner and a facility to view the lineage from source to result (and vice versa) through a suitable visualization tool.

Firms that fail to demonstrate data lineage to support qualitative reporting standards can find themselves in hot water. We've seen in audits that some G-SIBs were unable to fully reconcile regulatory reports back to their source data. Some firms were only able to escape penalties and fines by pushing back implementation deadlines. For others, their regulatory capital reserve was increased by the regulators.

> Proving data lineage is the digital equivalent of an accounting audit and should be approached with the same degree of rigor and discipline.

Leading Data Governance Concepts

Background

People, processes and technology comprise the majority of the investments financial institutions make in data governance. The relationship between data management and the business processes—and the highly-skilled people responsible for managing it—is a critical success factor. In the current environment, stakeholders place value on the knowledge of and control over data.

The Impact/Impact and Tactics to Consider/ New Considerations

Managers must ask themselves if their data warehouses are aligned to deliver upon three main elements of proper data governance: data quality, integration, modeling, security and privacy along with metadata and master data management.

Data warehouses should feature software or processes that manage the definition of data. Often, data warehouses service multiple stakeholders within an organization. Just as often, there may be disparate methods to define data schemas and elements in an accessible way. Within the confines of data definition is the classification of critical data elements—the fields that are essential to financial and risk calculations. Organizations should be monitoring these critical data elements for correct value ranges. They should also have methods to deal with outliers. Any volatility with critical data elements can cause a host of risk issues throughout the data use life cycle.

Regulators now ask organizations to understand and document the lineage of data through its use. Each end state calculation of a risk factor or a financial result is built on a stream of data that reaches all the way back to a source system or to manual input. The ability of a unified data architecture to document data lineage in a way that's quickly accessible to managers is not just a result of the data chaos emerging from the recession. Regardless of where data lives within the data bank, the mandate is that lineage must be documented indefinitely.

Putting It Together: Managing Data Lineage Ensures Provisioning of Certified Data

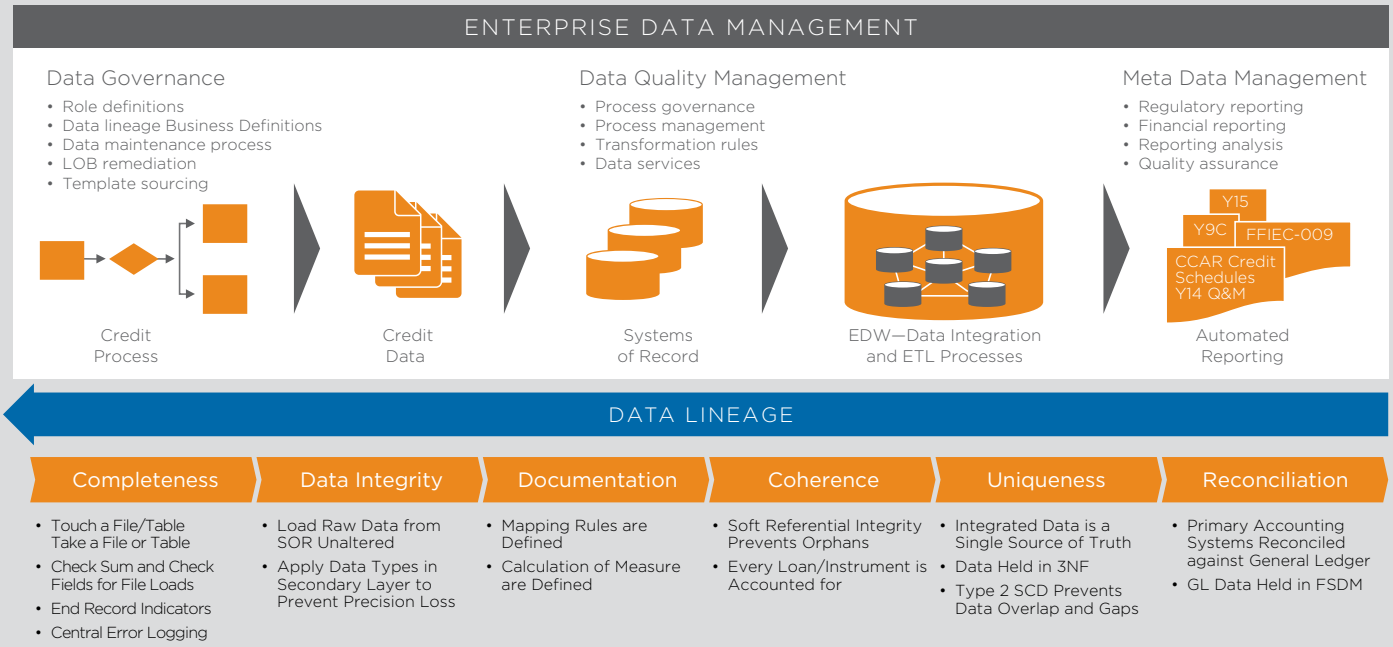

Figure 1.

Data change management connects critical data elements and lineage into organizational use. Documentation of and processes around how the data structure is changed over time can save millions of dollars. Many organizations find that data changed by one division has unintended consequences within another area's business processes. These changes take time and investment to research and remediate and can directly impact shareholder value and even customer service. The industry is making quick strides by creating data governance teams to efficiently manage change through organizational data management frameworks.

Summary

The internal and external requirements for transparency on data, systems, policies, processes, and documentation are more stringent than ever. Current policies aren't going away, but are evolving to become even more challenging in the future.

Without the right infrastructure in place, compliance with risk and financial processes can be extremely costly—and a big detriment to shareholder value due to the time, organizational involvement and expense involved in retaining compliancy. This also detracts from customer value, as potential investment rightfully allocated to innovation must be devoted to regulatory adherence.

However, an opportunity exists for companies to better leverage their data to become efficient in the delivery of compliance artifacts and process documentation, while concurrently optimizing internal and consultative resources.

An integrated, transparent data environment can support the data, analytic, and financial reporting needs of a resource-constrained organization under internal and external regulatory scrutiny. Systems that can self-monitor and allow business analysts to interact with them to gather either holistic or circumstantial facts (with minimal inquiry) fuel compliance and execution to support all lines of defense. This is the heart of the design and implementation of integrated data systems, and one which is becoming a means of fact-based, regulatory survival within the financial services industry.

An integrated, transparent data environment can support the data, analytic, and financial reporting needs of a resource-constrained organization under internal and external regulatory scrutiny.

End Notes

1. Basel Committee on Banking Supervision (2013), "Principles for effective risk data aggregation and risk reporting", BIS Report No. BCBS239, January 2013, http://www.bis.org/publ/bcbs239.pdf:
2. Lepus research, sponsored by SAS," Aggravation or Aggregation: Risk Data and Compliance", https://connections.teradata.com/docs/DOC-52651
3. Peter Weill, Stephanie L. Woerner and Mark McDonald, The Wall Street Journal, "IT Reuse Helps Businesses Thrive" http://www.wsj.com/articles/SB10001424052702304176904579111521673061960

10000 Innovation Drive, Dayton, OH 45342 **Teradata.com**

06.15 EB7088

TERADATA.