Operational Risk Management: Achieving Proactive Protection in a New Era
Executive Overview ................................................................. 2
Introduction ............................................................................. 3
Expanding Universe of Operational Risk ................................... 5
In Search of an Enterprise View ............................................... 6
Building a New Foundation ..................................................... 7
Charting a Course for Success .................................................. 8
Conclusion ............................................................................... 11
Executive Overview

Traditionally, financial services organizations approached operational risk management with an eye toward ensuring adequate capital to address “inevitable” events – those that are expected and unexpected – and satisfying regulatory requirements. However, times have changed in the post-financial crisis world. Today, firms are increasingly taking note of the positive impact that a comprehensive approach to risk management can have on both their reputation and profitability in ever-demanding times. They are also quickly realizing that their existing operational risk point solutions are simply not equipped to deliver the enterprise-wide visibility needed to achieve their goals.

To drive transformation, as well as meet growing regulatory and stakeholder demands, financial institutions require a modern and unified platform – consisting of a single data foundation; a robust data integration platform; a comprehensive set of risk management applications; and a powerful analytical layer with extensive reporting capabilities and actionable dashboards – that provides visibility into individual scenarios and vulnerabilities as well as overall operational risk. This functionality also extends into what we now call governance, risk, and compliance (GRC) by including compliance management, business continuity management, and that third line of defense, audit, into the picture. By providing a clear and single source of the truth for all those who need it in the organization, these combined tools – all using the same source data – allow a firm to better protect itself and its future from unexpected events and increasing regulations.
Introduction

The financial crisis of 2008 has fundamentally changed the way in which financial institutions view and manage risk. Regulations, crafted in response to unprecedented market events, are driving the transformation. While much of the focus has been on liquidity and capital risk, the industry’s approach to managing operational risk has also been evolving.

The Basel II Committee has defined operational risk as “The risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events.”¹ The focus in the late 1990s – when the Basel Committee began to address this issue – was on how much capital a bank required to cover its operational risk.

Banks identified and assessed risks on an individual basis, calculated potential losses, and set aside what they believed to be “adequate” capital to hedge against those risks and appease regulators. Firms created and deployed systems that mirrored and supported this approach. A typical operational risk system included functions for loss events and causal analysis, risk identification and assessment, control management and testing, key risk indicators (KRIs), and action plans. These systems were largely point solutions that assessed and managed each risk individually and relied heavily on spreadsheet-based analysis.

With the onset of the financial crisis, firms began to assess their organizations and business practices from top to bottom, including rethinking their approach to operational risk. Leadership, including boards of directors, began to see the benefits of an expanded focus on operational risk, which could span the following domains:

- IT Governance
- Financial crime
- Compliance
- Trading
- Business continuity
- Vendor/supplier networks
- Products
- Legal
- Health and safety issues
- Documentation issues
- Projects
- External Scenarios (geopolitical events, natural disasters)

Financial institutions, in turn, began to conduct risk and control self assessments (RCSAs) in earnest — as a tool for driving change — and started to recognize the value that good operational risk managers could deliver to their organizations.

The focus has now shifted from identifying sufficient capital to cover “inevitable” liabilities to proactively seeking an understanding of vulnerabilities and events across all of the firm’s operations and then working to improve controls and/or change processes and procedures to prevent them in the future. In essence, the practical definition of operational risk has evolved to encompass all threats to the successful achievement of corporate objectives, which might include protection of the firm’s reputation, the elimination of compliance breaches, fighting against financial crime, a 10% to 15% reduction in loss events annually, as well as lower costs leading to higher profits.

As executive management teams realize the positive impact that a strong operational risk methodology can have on public trust in an organization, as well as on a firm’s costs and profitability, they are also finding that many of their legacy point solutions cannot deliver the enterprise view, sufficient transparency, or analytical capabilities required to achieve these benefits. Therefore, financial institutions require new solutions to support their expanded focus on operational risk and compliance management.
Expanding Universe of Operational Risk

Managing operational risk can be compared to a popular carnival game in which a player uses a mallet to strike gophers as they pop up one after another. Just as the player thinks that he has the upper hand, the creatures pop up elsewhere. Today’s financial services institutions face more operational risk scenarios than ever before, and just as a firm appears to have current scenarios accounted for, new ones emerge. Some of the industry’s most prominent event scenarios include:

- Regulatory fines
- New regulations
- Leaked customer information
- Unauthorized trading
- Embezzlement
- Discriminatory practices
- Client misrepresentation
- Fiduciary breaches
- Business continuity failures
- Natural disasters
- Client misrepresentation
- Load fraud
- IT systems failure
- Failure of external suppliers

Financial crime is an especially vexing source of operational risk. It grows more prevalent and complex almost daily, fueled, in part, by the growing volume of electronic transactions. According to the 2011 ABA Deposit Account Fraud Survey Report, 100% of super-regional/money center institutions participating in the survey reported debit card, check, and automated clearing house (ACH) fraud in 2010. In the same biennial survey, respondents identified the leading threats as signature debit card fraud, customer victimization scams, cross-channel fraud, and automated clearing house (ACH) fraud – origins. Further, according to PricewaterhouseCooper’s (PwC) 2011 Global Economic Crime Survey, 45% of financial services organizations were victims of fraud in the past 12 months. While straight-through-transaction processing and channel proliferation have afforded new levels of efficiency for financial institutions and greater convenience for consumers, they are also creating new opportunities for fraudsters, as transactions are faster, do not require any human intervention, and are often “anonymous.”

As the incidence of financial crime increases, so do organizational costs, which include direct losses related to fraud, as well as the operational expenses associated with investigating and stemming it. In addition, damage to a firm’s reputation as a result of financial crime can have a lasting negative impact on the brand and bottom line. Under increased regulatory scrutiny, firms are quickly realizing that they do not always have the historic transparency they need to show why key operational decisions have been made and how and when risks and controls were comprehensively tested and, where appropriate, strengthened.

Regulatory compliance is another area of increased operational risk as oversight has proliferated and become increasingly prescriptive in the new millennium. For example, the U.S. Patriot Act, enacted in the wake of the September 11, 2001, attacks, introduced Know Your Customer (KYC) requirements, aimed at identifying and preventing money laundering that supports terrorist activities. Following the 2008 financial crisis, the United States Congress passed, and the president signed, the Dodd–Frank
Wall Street Reform and Consumer Protection Act, which is bringing hundreds of new requirements, including many of which remain in flux. Similarly, regulated firms across the globe are facing many pending and in-force regulations that require greater organization time, effort, and budget, and can lead to record corporate and personal fines when not met or breached. For example, starting in 2014, financial institutions will face a new layer of regulation as the Foreign Account Tax Compliance Act (FATCA) is slated to go into effect. Non-compliance with existing tax laws is already having a significant impact on companies, with a growing number of organizations facing steep fines and enduring costly convictions that, in one case, forced a firm out of business.

This increased regulatory burden comes with a hefty cost, including operational expenses related to compliance, fines associated with non-compliance as stated above, and, in the case of Dodd-Frank, missed opportunity costs as the result of new capital requirements. In August 2012, Standard and Poor’s estimated that Dodd-Frank could reduce pretax earnings for the eight largest complex banks by $22 billion to $34 billion annually.²

In Search of an Enterprise View

As financial institutions move toward an evolved approach to operational risk, they quickly realize that enterprise-wide visibility and transparency is essential. Not only do they need to have an enterprise-wide view of each type of risk, they also require a central location to collectively assess and manage the entire universe of operational risks across the organization. (See Figure 1.)

The challenge facing many banks today is that their legacy environments consist of a series of point solutions put in place at different times to manage specific types of operational risk, often just for specific lines of business. While some of the solutions might be integrated to varying degrees, they often cannot deliver an enterprise view of specific types of operational risk. More important, this approach precludes visibility into a firm’s collective operational risk, which limits its ability to quickly identify and address emerging issues. In addition, the point-solution approach creates increased IT complexity and risk, as well as incurs higher costs associated with licensing and maintaining myriad applications. The impact of this complexity becomes apparent when one considers that some global financial institutions may have upwards of 15 different GRC systems in place.

Building a New Foundation

Forward-looking financial institutions are looking to improve the management of risks, controls, obligations, and processes by creating a single, unified governance risk and compliance framework that breaks down legacy silos and yields a single organization-wide view of operational risk – a single source of the truth.

To deliver on these requirements, the unified environment must include a single data foundation; a robust integration platform; a comprehensive set of risk management applications; and a powerful analytical layer with extensive reporting capabilities and actionable dashboards. (See Figure 2.)

In addition to delivering enterprise-wide visibility that can help to stem operational losses and prevent damage to an organization’s reputation, this unified framework can help organizations to cut total cost of IT ownership by reducing point solutions and the need to license and maintain them. It also promotes data consistency and accuracy as well as improved collaboration across the compliance, risk management, anti-money laundering, financial intelligence unit (FIU), and audit functions, as well as across lines of business. Further, the approach expands insight into compliance requirements and the status of compliance enterprise-wide, which, in turn, can reduce the risk of regulatory fines.
Figure 2 – Unified data and technology break down silos.

Furthermore, as firms look to strengthen their three lines of defense principle, it is essential that all those with risk, compliance, and audit responsibilities, not just those in the risk, compliance, and audit departments, have access to the right tools and consistent data that a unified platform and a comprehensive eGRC solution can deliver.

A unified platform can also be instrumental in helping organizations to implement the advanced measurement approach (AMA) methodology for capital calculation under Basel II, the most sophisticated and complex of the four options that banks can use to calculate regulatory capital for operational risk. The AMA can afford banks several benefits, including a reduction in the amount of regulatory and economic capital that it must set aside. Achieving AMA certification, however, requires extensive data, as well as sophisticated modeling and analysis capabilities that only a unified platform can support.

**Charting a Course for Success**

Where should a financial organization begin its operational risk environment transformation journey?

Organizational support is critical and must emanate from the executive suite. It cannot stop there, however, as the chief risk officer must also involve and cultivate leadership from his/her operational risk, compliance risk, and audit teams, as well as lines of business leads. As with any successful
enterprise project, stakeholders must be engaged early and given meaningful involvement throughout the initiative.

It is also necessary to assess the organization’s current operational risk capabilities. The team assigned to the operational risk transformation initiative should explore the following:

- What is working in terms of the organization’s operational risk strategy as well as supporting systems?
- What are the weaknesses and where could the organization benefit from best practices and expanded capabilities?
- What are the findings of the organization’s most recent RCSA, and what areas does it identify for action?
- Can the organization easily and with full transparency show regulators a comprehensive list of assessed/audited risks, controls, issues and corrective actions, decision making processes, and appropriate challenges, as well as the latest state of compliance with regulations – from both an enterprise and local angle all using one source of data?
- What is the vision for the organization’s operational risk strategy?

The answers to these questions will illuminate the path forward.

In determining technology requirements and choosing a platform that can deliver enterprise-wide visibility, organizations should follow a similar evaluation process. Important considerations include:

- **Does the solution have a single data infrastructure and unified data model purpose-built for the financial services industry?** A single data foundation and model are critical to enabling a holistic and accurate view of each risk type and assessing overall operational risk across the enterprise.
- **Is the solution flexible?** The platform should be able to expand to support new types of risk as they emerge, as well as new regulatory and internal compliance requirements. In addition, it should enable an organization to optimize its existing technology investment as it wishes. Therefore, the platform should be open to facilitate the integration of existing operational risk point solutions or key data from existing financial crime systems, such as anti-money laundering or fraud information, into the infrastructure on a short-term or permanent basis.
- **Can the solution deliver insight at various levels?** The platform should enable an organization to visualize and assess risk from several different perspectives, such as by individual type of risk, within a certain line of business, in a specific geographic region, or enterprise-wide across all types of risk, as required.
- **Does the platform deliver comprehensive functionality?** A unified platform must support the wide range of operational risks that today’s institutions face to enable financial services organizations to advance their operational risk management capabilities. The solution should also include functionality that supports the broader operational risk management function, such as components for:
- Loss and incident collection
- Insurance policies and claims
- RCSA
- Top risk scenarios
- KRI
- Central libraries for risk, controls, insurance policies, questions/questionnaires, vendors, products, IT system information, and compliance information, including data on laws, regulations, and internal policies
- Issues and action plans
- Change management projects
- Business unit risk profiles
- Advanced compliance management
- Business continuity management
- Audit management

• **Does it enable real-time monitoring and analysis?** The platform must enable real-time monitoring capabilities to support rapid response in areas in which it is required, such as financial crime and compliance management, where online access and authentication are essential for earlier identification of potential fraud schemes.

• **Does the application strengthen the three lines of defense model?** The platform must support the three-lines-of-defense model by providing effective traditional risk and compliance oversight functions and features and by delivering new business-focused features, such as the business unit risk profile, which makes it easy for the first-line of defense teams to access all the information and features they need to fulfill their obligations.

• **What type of security and access control does it provide?** Operational risk data can be extremely sensitive. Not every member of the compliance network requires access to all types of information. For example, it would not be wise to make details of how a fraud was perpetrated widely available or even to know how another business unit was faring in terms of its risk assessments. As such, the platform should have advanced security, which enables the company to define access based on roles and other criteria.

• **What type of analytical and reporting capabilities does the solution provide?** Advanced analytical capabilities deliver the insight that organizations require to make sense of the vast stores of operational risk data that they have within their enterprises. These capabilities must be easy to use so that line-of-business personnel can access the information they need without relying on the IT team for support. This capability enables more timely analysis and insight. As important, analysis and reporting must be flexible to provide a variety of users with the level of information they require. Dashboard capabilities that can be configured for various roles, such as operational risk personnel, audit teams, compliance teams, and lines of business managers also can improve insight and action.
Conclusion

The stakes are high for today’s financial institutions when it comes to risk management. Organizations that adopt a proactive, comprehensive and holistic approach to operational risk management, and invest in the unified technology infrastructure required to support it, stand to reap important short- and long-term benefits, which include reduced operational losses, fewer regulatory fines, and improved public confidence and trust in the institution — all of which translate to a positive impact on the bottom line.