Managing regulatory change

Deploying a flexible, future-proof system to gain deep insight into corporate governance and adapt to new risk and compliance challenges in a fluctuating globo-political landscape

Contents

Executive overview

The passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act introduced long-awaited financial reform in the United States, but it has also created additional uncertainty for companies that are trying to define persistent governance, compliance and risk initiatives. With the continuing evolution of the regulatory environment, Dodd-Frank illustrates the growing challenge of managing regulatory change.

The wide scope of the Dodd-Frank Act impacts virtually all aspects of financial services, encompassing banks and other systemically significant institutions, both public and private. It will largely fall upon regulatory agencies to transpose the intent of this law into rules and regulations that will govern how bank holding companies and other financial services institutions are impacted.

Dealing with the changing regulatory environment

In responding to Dodd-Frank, companies conducting business in the US are subject to regulatory oversight that impacts actions internally and externally for a diverse range of business processes.

Over the past decade, the US government has enacted or significantly revised momentous regulatory frameworks covering everything from health records confidentiality (Health Insurance Portability and Accountability Act [HIPAA]), corporate auditing (Sarbanes-Oxley Act [SOX]), homeland security (USA PATRIOT Act), and more.

Dodd-Frank has provided preliminary authorization for increased resources that ensure that its scope and enforcement activity will expand greatly over the next five years. However, work has quickly commenced on elements that can be implemented in relatively short order. Treasury Secretary Timothy Geithner, who also chairs the newly formed systemic risk council of U.S. regulators, promised that the board would move quickly and seek “to avoid the ‘glacial pace’ of most oversight changes and cut through layers of ineffective past efforts.”[1]

This demonstrates the imperative for executive management to evaluate the short-term and long-term implications on their governance, risk management and compliance strategies and the need to ensure their organizations can effectively adapt to manage regulatory change.

As Dodd-Frank rulemaking proceeds, organizations that react to each new rule and regulatory requirement with islands of technology and resource investments will find themselves facing severe consequences such as high costs and operational inefficiencies, and will likely further deter the horizontal integration of effective operational risk management strategies.

Inevitably, there will be a lot of overlap between information requests from the different regulatory entities. The ability to handle these requests, along with those necessitated by internal audit, calls for technology and policies that minimize the processes needed to meet those requirements. The interdependencies of different business organizations and functions are a critical consideration in reducing costs, increasing efficiency and creating transparency in enterprise risk management.

Operational risk: Lessons learned

Operational risk has always been a key factor in modern commerce, but today's focus on ensuring optimal business performance while reducing loss, protecting investors and the corporate brand, has forced executives to re-emphasize its importance. The Basel Committee defines operational risk as, "The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events,"[2] and pundits have extended this definition to include suppliers as well.

In response to Basel II, many forward-thinking organizations in the banking sector have been successful in implementing a consolidated approach to manage operational risk. Basel II expounds upon the already complex "three pillar" concept introduced in Basel I, giving banks some flexibility in refining their compliance strategy. These companies have been able to deploy an integrated system capable of managing the operational risk process from end-to-end with solutions for handling such disparate requirements as risk and control self-assessments (RCSA), loss events, capital reporting, etc.

However, the financial meltdown of 2007-2010 has further highlighted the importance of better managing operational risk and how far many organizations are from being able to effectively do so. Andreas A. Jobst, an International Monetary Fund (IMF) economist, concluded in a recent article that, "institutions are at different stages of systems development and show considerable dispersion in [operational risk management] practices while falling short of integrating operational risk as a horizontal process."[3]

Many existing risk and compliance management systems are not equipped to capture complex interdependencies of a multitude of factors that span global regions, lines of business and functional organizations. An effective system that meets the challenges of today and is prepared for the obstacles of tomorrow must automate the process of identifying, measuring and monitoring risk, combining all risk data – risk and control self assessments, loss events, scenario analysis, external losses, key risk indicators, issue and policy management – into a single integrated solution. This type of infrastructure is also instrumental in effective regulatory management.

The Dodd-Frank example

While the overall thrust of Dodd-Frank is to reduce systemic risk, the legislation has also established a number of new entities charged with collecting data, writing or revising rules and/or monitoring business activity:

- The **Financial Stability Oversight Council (FSOC)** is a regulatory board established under the Dodd-Frank Act and is charged with monitoring systemic risk within the U.S. financial system. The Council will collect risk data from various sources, including federal and state financial regulatory agencies and the newly created Office of Financial Research. Consisting of the heads of existing regulatory agencies, the Council may recommend that a member agency adopt stricter standards for the firms it regulates in order to mitigate systemic risk[4].
- The **Office of Financial Research (OFR)** is charged with collecting risk data from financial services institutions at the behest of the Council. Bloomberg Businessweek reported that, armed with subpoena power, the OFR is already noted for the "unusually strong powers Congress granted it to force financial companies to turn over confidential information and help spot potential market blowups. In a nod to its abilities to peer into the uncharted depths of the financial system, lobbyists are calling it the CIA of financial regulators."[5]

- The act also mandates **Risk Committees** for all publicly traded bank holding companies with assets of $10 billion or more and certain publicly-traded and systemically significant non-bank financial services companies. Additionally, the Federal Reserve is empowered to require the same committees for bank holding companies with less than $10 billion in assets. These Risk Committees are responsible for enterprise-wide risk management oversight and practices and are required to include at least one risk management expert with "experience in identifying, assessing and managing risk exposures of large, complex firms"[6].
- The Dodd-Frank Act also created a new federal **Consumer Financial Protection Bureau (CFPB)** that will police loans and financial services products that banks and others sell to consumers.

Managing the additional relationships and requirements that stem from these agencies requires organizations to abandon antiquated filing systems and desktop applications for an agile solution that is built to handle complex interactions. Workflow support, monitoring, notifications and reporting ensure that internal teams can stay on top of the compliance process at every stage and are prepared to respond to requests in a timely fashion.

Managing regulatory change

In the wake of Dodd-Frank passage, Chris McClean of Forrester Research commented that there are nearly 200 regulatory changes still on the US federal agenda that span industry verticals such as finance, healthcare and consumer protection[7].

How can organizations prioritize and cope with such a large number of compliance concerns and also prepare for future regulatory change? Many companies are turning to governance, risk and compliance (GRC) software to establish a steadfast infrastructure for managing regulatory change, regulator interaction and the end-to-end policy lifecycle.

Policies establish the culture, values, ethics and duties of a corporation. Organizations that take a provisional approach to managing and communicating policies face significant risk to their business. The key to effective compliance and policy management is constructing a formalized and efficient mechanism for the communication, tracking and attestation of regulatory change so that business are equipped react quickly to change – particularly in a complex and mercurial regulatory environment.

Regulatory mandates, external risk factors and operating processes also necessitate the adoption of a unique set of policies to meet those requirements. All too often, organizations rely on a three-ring binder of dusty policies that no one has read. Some companies may have upgraded to intranets and Microsoft Word documents, but the core problem persists: disparate and disconnected systems simply cannot manage the breadth and variety of policy and compliance initiatives vital to modern business performance. In order to foster an enterprise-wide culture of governance, risk and compliance management, policy needs to be visible and actionable to organizational stakeholders.

As regulatory pressures continue to mount, organizations that adopt a more practical regulatory management approach will be able to decrease costs and overall complexity while gaining valuable insight into the risks that could affect corporate performance in the form of legal action, fines and penalties, or a decline in company/brand loyalty.

Dodd-Frank has highlighted the potential that regulators have to interact with many different divisions and functions within an organization. It is becoming increasingly important for companies to efficiently manage these interactions, associated internal workflow processes, and the entire life cycle of the resulting documentation. To meet the potential volume of such as inquiries, submissions, filings, exams and audits, it is paramount that companies create an automated enforcement and monitoring infrastructure to ensure that the right interactions take place, deadlines are adhered to, and company policies are accurately represented.

Architecting the right approach

For each new regulation or risk discipline, companies typically implement a new technology solution narrowly focused on the specific mandate. This fragmented approach limits an organization's ability to streamline risk and compliance processes and reduce costs. It also obscures the opportunity to integrate risk and compliance and gain a holistic view of the firm's risk landscape, leaving them ill-prepared for managing the growing number of policies and regulations that are becoming integral to enterprise operations.

In order to meet the regulatory management challenge and the mounting requirements for risk exposure data, organizations need to implement internal infrastructure and processes that provide full transparency and reporting for its board of directors and risk committee, as well as external regulators.

Effective information architecture should:

- Provide flexibility to extend and adapt to new regulatory demands without requiring extensive rewriting or customization.
- Ensure the ability to quickly and accurately collect, distribute and report on risk and compliance data so that decision-makers have visibility across the enterprise.
- Implement a process lifecycle for communicating policies, tracking attestation, monitoring metrics and relating internal policy processes to overall risk, issue management, and other governance, risk and compliance areas.

IBM® OpenPages® Policy and Compliance Management

To meet the challenges posed by the dynamic environment of regulatory change, it is essential that businesses deploy or enhance existing governance, risk and compliance solutions. Decision-makers need to establish a programmatic framework for communicating changes to regulations and managing the internal regulatory process so they can react quickly to each new policy or mandate that is put in place.

Just as important is the need for systems, policies, and automation in managing relationships with external regulators such as inquiries, submissions, filings, exams and audits.

The IBM® OpenPages® GRC Platform serves as the foundation for enterprise governance, risk and compliance management efforts through its ability to unite an organization's risk and compliance initiatives into a single management system.

With solutions for Financial Controls Management, Operational Risk Management, IT Risk and Compliance, Internal Audit Management, and Policy and Compliance Management, the OpenPages GRC provides a modular and integrated approach to governance, risk and compliance, enabling organizations to:

- Manage risk and compliance for multiple regulations, including Basel II, Solvency II, SOX, and SOX-like requirements around the globe, privacy, data privacy requirements, industry regulations and more.
- Understand the interdependencies between risks and controls that are shared across processes, departments, business units and geographies.
- Implement a unified and simplified approach to enterprise GRC management to reduce redundancy, minimize complexity and maximize efficiency.

OpenPages PCM is an integrated module that enables organizations to react quickly to complex and evolving regulatory mandates like Dodd-Frank with solutions for:

- **Regulatory Change Management** – lets users easily communicate, track and manage regulatory change and enables quicker reactions
- **Regulator Interaction Management** – provides workflow enablement to help users prepare for and manage complex regulator interactions
- **Policy Lifecycle Management** – allows for policies to be easily managed throughout all life cycle phases including development, review/approval, communication, training/ assessment, maintenance and monitoring

IBM OpenPages enables organizations to gain deep insight into all aspects of enterprise-wide governance, risk and compliance with an integrated solution that can seamlessly adapt to unique risk management methodologies, taxonomies and business practices. Organizations are able to share processes, risks and controls between business units to reduce complexity, eliminate duplication of efforts, increase effectiveness and understand interdependencies between key business processes.

IBM OpenPages meets risk and policy challenges head-on with a highly configurable solution that supports an organization's specific enterprise risk management methodology, without having to write custom code. The result is that companies can embed risk management into the business and vastly improve performance over time.

About IBM Business Analytics

IBM Business Analytics software delivers complete, consistent and accurate information that decision-makers trust to improve business performance. A comprehensive portfolio of business intelligence, predictive analytics, financial performance and strategy management, and analytic applications provides clear, immediate and actionable insights into current performance and the ability to predict future outcomes. Combined with rich industry solutions, proven practices and professional services, organizations of every size can drive the highest productivity, confidently automate decisions and deliver better results.

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
May 2011

[1] Rebecca Christie, *Geithner Says Financial Oversight Council to Offer 'Road Map'*, Bloomberg Businessweek, August 2, 20100

[2] Secretariat of the Basel Committee on Banking Supervision, *The New Basel Capital Accord: an explanatory note*, January 2001.

[3] Andreas A Jobst, *The Credit Crisis and Operational Risk – Implications for Practitioners and Regulators*, Journal of Operational Risk, Vol. 5, No. 2, Summer 2010.

[4] H.R.4173 – Dodd-Frank Wall Street Reform and Consumer Protection Act, http://www.opencongress.org/bill/111-h4173/text.

[5] Robert Schmidt, *The Treasury's New Research Office*, Bloomberg Businessweek, September 2, 2010.

[6] H.R.4173 – Dodd-Frank Wall Street Reform and Consumer Protection Act, http://www.opencongress.org/bill/111-h4173/text?version=enr&nid=t0:enr:1307.

[7] Many companiesMcClean, Chris. *Think You Know About All The Big US Government Regulations Coming Up? All 191 Of Them?* Retrieved 4/15/2011 from http://blogs.forrester.com/chris_mcclean.