A Good Offense is the Best Defense: Managing Regulatory Compliance with GRC
A Proactive Strategy toward Regulatory Compliance

An ever-evolving regulatory environment coupled with increasing oversight pressure is challenging organizations to manage and comply with a continuous wave of new regulations. Congress enacts thousands of pages of legislation annually, and many of these (see Bracing for Regulatory Impact on the following page), such as the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), have compelled organizations to focus on the regulatory compliance aspects of these acts using already strained human and financial resources.

According to a recent Economic Intelligence Unit/KPMG survey,¹ many companies find it difficult to keep pace with the rate of new regulations and compliance. As a result, a frequent response to a new regulatory requirement is to add an extra process or function, an ad hoc approach that may address the immediate issue but can lead to overlapping responsibilities, inconsistent processes, and duplicated efforts. And costs. Indeed, almost a third of the global executive respondents² say that they spend more than 6 percent of their organization’s annual revenues on governance, risk, and compliance (GRC) activities. There is also near-universal agreement that the cost of these activities is rising. Over the past two years, 89 percent say that the cost has increased, and 84 percent expect it to grow further over the next two years.

One reason for this cost is the additional time and staff required to understand and address the complexity of some of the more recent regulations. The Dodd-Frank Act is a prime example. Consider that all public companies must comply with the SEC’s final rule on the Dodd-Frank Act’s whistleblower protection program, which is outlined in a 305-page directive that is included in the Investor Protection section.³ Investor Protection is just one of 16 provisions of the Act. Consider the time and attention companies will devote to interpret and comply with the Act in its entirety, if one rule in one section requires more than 300 voluminous pages of review.

And while the Dodd-Frank Act may greatly impact both financial and non-financial services companies alike, it is just one example of regulatory reform that is changing the way organizations will be required to conduct their businesses.⁴ Major public policy changes like the Dodd-Frank Act are occurring in financial services, healthcare, energy, and other areas. Such reform has the potential to affect a broad cross section of companies and industries, imposing additional requirements for transparency and compliance obligations and requiring new governance oversight processes. Moreover, increasing regulatory activity relating to data protection, privacy laws, and global business practices is also posing new risks.⁵

¹ The Convergence Evolution: Global survey into the integration of governance, risk, and compliance, February 2012, KPMG International, in co-operation with Economist Intelligence Unit.
² The survey was completed by 177 executives globally, representing a wide range of industries and regions.
⁴ “Dodd-Frank: Beyond Financial Services – The implications and effects on nonfinancial service companies,” August 2011, KPMG LLP
⁵ Public Policy Alert # 12, Legislative complexity challenges traditional business and compliance strategies, November 2011, KPMG Institutes (www.kpmginstitutes.com)
The expense associated with these compliance efforts can directly impact an organization's bottom line and, if the added layers of people and process are ineffective or inefficient, may not significantly reduce the risks of noncompliance. But woe to those organizations that choose to ignore these risks, which may include damaged reputation, loss of revenue, decreased shareholder value, hefty fines and sanctions, as well as personal liability for company leaders. Put simply: Organizations may be playing a form of "regulatory roulette" by using an ad hoc – as opposed to holistic – approach to regulatory compliance.

The Dodd-Frank Act is just one regulatory hurdle challenging industries. As regulatory reform begins to reshape many industries, organizations will need to maintain a dual focus on business performance and regulatory compliance in an environment in which both outcomes must be managed strategically and with agility. Industry leaders will need to strengthen their approach to measuring, managing, and mitigating risk. Organizations will also need a disciplined process for managing the entire spectrum of risks more effectively, including new risks associated with information and data management, as outlined in the recent Securities and Exchange disclosure guidance regarding cybersecurity.\(^6\)

The good news is that business leaders can begin the process by asking themselves (see Questions Businesses Should Ask about Managing Risk and Regulatory Reform on the following page) about their capacity to manage such risks now and going forward. The better news is the availability of a holistic approach to governance, risk, and compliance.

---

6 Public Policy Alert #13, Focus on information protection intensifies as market forces and regulatory disclosure requirements increase, December 2011, KPMG Institutes (www.kpmg institutes.com)
Questions Businesses Should Ask about Managing Risk and Regulatory Reform

- Is our governance structure appropriately supported by our risk and control framework?
- Do we have the right competencies to analyze and operationalize the implications of reform or additional regulations?
- Do we have an inventory of all regulatory requirements that our organization needs to comply with now?
- Do we have an ongoing process for interpreting new regulations?
- Are we ready to restructure the business model, while managing the potential for increasing risks?
- How well is the compliance group integrated into other oversight functions?
- Do we have the right information for decision making, reporting, and compliance?
- Do we have the right controls to address fraud, waste, and abuse as well as internal controls over reporting?
- Do we have a process for evaluating the effectiveness of controls and responding to deficiencies noted by regulatory agencies?
- How can we use GRC as a way to help our organization achieve the highest levels of business integrity?

A Holistic Approach to GRC

One solution to proactively manage regulatory compliance is by preparing for new regulations rather than reacting to them. A holistic approach to governance, risk, and compliance (GRC) enables a proactive stance by bringing both complex and disparate risk and compliance activities into alignment with corporate strategy and improving the efficiency and effectiveness of those activities.

GRC can be defined as a strategic approach to integrating risk management, regulatory compliance, controls, assurance structures and processes, and intelligently using IT and data management structures supported by a strong organizational culture.

By proactively managing GRC, an organization can recalibrate governance, monitoring, and operating processes to help ensure regulatory compliance. The overarching goal is to create an integrated view of risk that breaks down across the many silos that may exist throughout an organization to enable more effective compliance before issues arise, and promote smarter, more informed business decisions.

A Strategic View of Risk and Compliance

A holistic approach to GRC encourages a strategic view of risk and compliance, which is necessary to proactively manage the wave of regulations that exist today. An organization can begin its proactive approach by taking an inventory of all the regulations affecting the industry/firm and assessing its exposure.

The organization will then need to unify the fragmentation of structures, systems, and processes built over time in response to prior regulatory and business changes. This involves identifying and reducing overlapping and redundant policies, assessments, controls, reports and tests set up to satisfy multiple regulations or mitigate risks and then consolidating all of these efforts going forward.
By evaluating information surrounding policies, risks, and controls (see above), an organization can map regulations to policies, objectives, risks, and controls to show evidence of compliance. New regulations, or changes to existing ones, can be accommodated in a timely, cost efficient way with suitably skilled and capable resources. In some cases, the same controls can be used for different regulations, creating a more effective and cost-efficient way to help ensure compliance for new regulations, as necessary.

An Example of a Holistic GRC Model
The ability to proactively manage the influx of new regulations will depend heavily on the structure, role, and communication of the compliance function within an organization. For instance, KPMG has created a holistic GRC model to equally balance important efforts to optimize risk, strengthen culture and behavior, enhance governance and infrastructure, and help ensure enterprise assurance. Effective operationalization of risk management (including compliance) in business processes lies at the core of KPMG’s GRC model and is essential to reducing the complexity of managing risk and compliance in a multi-regulatory environment.

As a compass for an organization’s risk and compliance activities, the model offers a framework to unite and direct processes to support corporate strategy, allowing the specific components of governance, risk management, and compliance to be evaluated and targeted for reengineering in a modular manner. The model does not propose a centralized approach to risk management. Rather, it recognizes that risk is often managed closest to the point of origination—specifically, the business line and business processes—that are operated by people who know the related risks.

KPMG’s Holistic Model
A Good Offense is the Best Defense: Managing Regulatory Compliance with GRC
Driving Business Value

In this era of unprecedented regulation, resilience is the key to organizational survival. And GRC is the key to driving resilience, a state in which business performance and regulatory compliance are managed strategically and with agility. A holistic GRC model can add value by helping an organization reduce the risks of regulatory noncompliance by:

- Aligning GRC to organizational strategy and mission
- Supporting informed decision-making driven by robust governance structures, level-appropriate reporting dashboards, and intelligent use of IT and data management based on a set of agreed-upon guiding principles
- Enhancing consistency, transparency, and operational efficiency by rationalizing overlapping risk management efforts, controls, and assurance structures and processes through a common set of risk taxonomy, issues management, and reporting processes

- Supporting an efficient response to the challenges posed by the evolving risks and rapidly changing regulatory requirements based on consistent and timely analysis of risk drivers and performance metrics from business functions—including the operations, finance, compliance, and regulatory teams
- Fostering a culture that understands and embraces GRC as a source of competitive advantage
- Orchestrating the four intrinsically linked components—the enterprise risk profile; culture and behavior; governance, organization, and infrastructure; and enterprise assurance.

The model provides a structure for aligning risk management and compliance activities with governance efforts, organizational culture, and enterprise assurance and reporting. Thus, the model supports a multitude of board and management needs while providing valuable feedback to the strategic decision-making processes. Resilience—or the ability to drive business performance and achieve regulatory compliance in an environment in which these two outcomes are managed strategically and with agility—is not an end-state but a continued goal, driving improved compliance and performance even in the most challenging regulatory environments (see above Driving Business Value).

Within the model, four key components of equal importance (see Four Key Components to the right) must be in balance to enable resilience. By aligning these four components with the goal of managing regulatory compliance, organizations can proactively manage compliance requirements in a cost-effective and efficient manner.

The model adds value by providing an efficient manner in which to keep organizations informed of new developments and help executives and board members prepare and understand the full impact of public policy and regulatory reform affecting their industry.

Four Key Components of KPMG’s Holistic Model

- **Risk profile** – Understanding and quantifying risks facing the organization can help the organization enhance coverage at the lowest cost;
- **Culture and behavior** – Embedding a culture and behavior of risk management within everyday behavior can help ensure the possibility that money be allocated appropriately and effectively;
- **Governance, organization, and infrastructure** – Giving oversight on business processes and decision-making will help ensure that regulation is addressed in the most cost-effective manner;
- **Enterprise assurance** – Evaluating, monitoring and reporting on the effectiveness of controls enables measuring response to regulatory change.

The structure of the model offers a way for organizations to better evaluate their overall risk profile as well as the effectiveness of their risk management and compliance programs before problems occur. Overall, the goal is to help organizations achieve the highest levels of business integrity in a proactive manner through sound corporate governance, internal controls, and transparency by increasing efficiencies and reducing silos.
A Good Offense is the Best Defense: Managing Regulatory Compliance with GRC
Case Studies: GRC in Action

A Fortune 500 power and utilities company

A Fortune 500 power and utilities company was interested in implementing an integrated risk assessment across the organization to proactively identify key risks and direct actions to mitigate those risks. The company wanted to replace an existing software system that supported the Sarbanes Oxley (SOX) function and leverage the testing and assessment work that was performed across multiple groups to gain efficiencies.

A team of KPMG professionals helped develop a common language of risk and methodology to assess risk to ultimately enable the implementation of a GRC application. The team worked closely with their Chief Risk Officer (CRO) and business workstreams to help refine their business requirements and develop a common language of risk, including the organizational, process, risk, and control taxonomies. KPMG brought in subject matter professionals with environmental, regulatory, compliance and other financial risk experiences (credit, market and liquidity) as needed to assist the business in refining its requirements. In addition, the team worked with the client and its IT vendor to develop a ‘proof of concept’ showing how the business requirements can be attained in the application. The team is also instrumental in the design, development, and delivery of user training.

By providing a clear view of business requirements and defining a common language of risk, the company’s oversight functions are now able to proactively manage risk and regulatory compliance at an appropriate level—without losing sight of the bigger picture. Moreover, having a clear view of business requirements allowed the company to make key decisions that increased the efficiency and functionality of the GRC IT application.

A large global financial services company

To lessen the burden on its business units, a large global financial services company wanted to improve its controls and compliance functions to achieve greater leverage across its business units while streamlining various review processes. The company’s objective was to drive efficiencies by rationalizing duplicate efforts and tools and make any necessary organizational, process, or tools adjustments.

KPMG assisted in making necessary recommendations to achieve the company’s convergence goals. KPMG compiled a convergence team supported by subject matter professionals across different functions. The team helped establish convergence guiding principles and assisted in defining business requirements. The team identified convergence opportunities while recognizing functional improvements and provided improved foundational elements that can be shared across functions for a consistent and integrated process.

As a result, the team was able to help streamline the company’s controls and compliance functions, lessening the burden on the business by introducing master planning for activities supported by optimized risk assessments, knowledge and issues management supported by a common language, and converged testing and monitoring. In addition, the company was able to enhance its resources skills and capabilities through centralized risk and control training across the oversight functions. By taking the necessary steps at the onset, the company was able to improve its compliance function so that it could effectively manage regulatory compliance and help mitigate future risks.

An integrated approach to managing governance, risk, and compliance activities.
Moving Forward with GRC

A GRC strategy that is well planned and executed can significantly simplify processes, reduce costs, and ease the compliance burden associated with increasing regulations and public policy. Yet, while many organizations want to achieve GRC convergence, they may be uncertain where to begin. To get started, an organization should consider the following key steps:

1. **Secure** buy-in and endorsement from the executive leadership team.

2. **Build** a governing structure and develop a steering group comprised of leaders from each of the oversight functions included in the convergence efforts, headed by a senior-level leader.

3. **Consider** all key internal stakeholders and regulatory regimes in the convergence effort and identify all requirements to be accommodated at the outset.

4. **Establish** guiding principles to ensure alignment with strategic objectives, cross-company buy-in, and consistent progress.

5. **Begin** with well-defined risk assessment processes.

6. **Establish** a clear change management plan and implement it throughout the program.

7. **Take** a holistic view across the organization to identify opportunities beyond converging control and compliance to other organizational and process changes that may benefit the organization.

8. **Think** people, process, and data: don’t let a tool or technology alone drive the convergence process.

---

*A dialogue with a company’s Audit Committee may also be useful, especially since Audit Committees are spending more time evaluating legal and regulatory issues, as outlined in the 2011 Public Company Audit Committee Survey – Highlights, Audit Committee Institute (www.kpmginstitutes.com)*
Contact us

To find out more about how KPMG can help you manage GRC efforts within your organization, please contact:

**John Michael Farrell**  
Partner and Global Leader, Governance, Risk & Compliance  
T: (212) 872-3047  
E: johnmichaelfarrell@kpmg.com

**Deon Minnaar**  
Partner and National Leader, Governance, Risk & Compliance  
T: (212) 872-5634  
E: deonminnaar@kpmg.com

**Angela Hoon**  
Principal, Advisory Services  
T: (267) 256-1970  
E: ahoon@kpmg.com

**Jesal Asher**  
Principal, Advisory Services  
T: (212) 954-3041  
E: jesalasher@kpmg.com

**Emad Bibawi**  
Partner, Advisory Services  
T: (212) 954-2033  
E: ebibawi@kpmg.com

**Amy Matsuo**  
Principal, Advisory Services  
T: (919) 380 1509  
E: amatsuo@kpmg.com

**Lynn McKenzie**  
Partner, Advisory Services  
T: (213) 955-8614  
E: lmckenzie@kpmg.com

**Jil Polniak**  
Partner, Advisory Services  
T: (408) 367-7616  
E: jpolniak@kpmg.com

**Mark Twerdok**  
Partner, Advisory Services  
T: (412) 232-1599  
E: mtwerdok@kpmg.com

**Kreg Weigand**  
Partner, Advisory Services  
T: (612) 305-5581  
E: kweigand@kpmg.com

**Michael Wilson**  
Principal, Advisory Services  
T: (713) 319-2291  
E: michaelwilson@kpmg.com

kpmg.com

The information contained herein is of general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should rely upon or use such information as the basis for taking any action or making any decision and any such action or decision should be based upon appropriate professional advice and a thorough examination of the particular situation.

© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. Printed in the U.S.A.