# Governance, Risk and Compliance: 4 Key Drivers

Making the business case for an integrated and truly pervasive governance, risk and compliance (GRC) solution can be daunting. GRC is evolving, and putting accurate numbers around a moving target is no easy task. What's more, calculating the real financial and reputational cost of preventing an incident remains elusive.

Thursday, May 29, 2014

By Brenda Boultwood



Making the business case for an integrated and truly pervasive governance, risk and compliance (GRC) solution can be daunting. GRC is evolving, and putting accurate numbers around a moving target is no easy task. What's more, calculating the real financial and reputational cost of preventing an incident remains elusive.

Consequently, making a compelling argument for GRC often requires either a crisis or a damaging incident - e.g., a loss, a fine or a reputational impact - to focus an organization's attention and resources in a way that truly matters.

*Brenda Boultwood is the senior vice president of industry solutions at MetricStream*

In spite of the difficulties in building a business case, leading companies recognize that there are advantages to adopting a holistic GRC solution. The reason? In the midst of today's cloudy, global, virtual, social and mobile world, a strong GRC technology ecosystem provides organizations with the qualitative and quantitative data that can strengthen business decisions in order to meet current challenges and pursue future opportunities.

Given the investment of capital and organizational resources required to implement and sustain a pervasive GRC program, it's perfectly understandable that many organizations subject GRC to the rigorous scrutiny of a cost-benefit analysis. But as organizations attempt to measure the ROI of GRC, there is a single question that must be included in every analysis: What are the long-term costs ofnothaving a holistic and integrated GRC system?

This article breaks down the four components that should be driving your organization's GRC cost-benefit analysis. While these benefits are qualitative, the adoption of a GRC program will help an organization quantify them.

**Understanding the GRC Investment**

There's no doubt that implementing a comprehensive GRC framework involves a substantial expense. According to a report from Forrester (http://www.forrester.com/Build+The+Business+Case+For+A+GRC+Platform/fulltext/-/E-RES56677?objectid=RES56677), the initial costs (including software, hardware and implementation services) vary widely, ranging from $200,000 to $600,000. But the total cost of ownership (TCO) extends beyond software and hardware components to encompass a range of supplemental expenses related to consulting, training, customization, maintenance, upgrades, security and operations.

In addition, an effective and pervasive GRC program should be as dynamic as the business environment it's meant to serve. This means that GRC is not simply a technological framework but also an ongoing process that may require an expansion of scope and, consequently, an increase in cost. This is especially the case as global regulatory and compliance regimes continue to mature, and as organizations expand to new market segments, each with their own specific set of GRC requirements.

Despite the initial and projected expense, GRC is perhaps best viewed as an investment. Making an investment in an integrated GRC program can certainly yield numerous benefits that, while often difficult to measure, provide organizations with significant long-term ROI.

Specifically, the GRC value proposition lies in its ability to improve risk management efficiency and ensure compliance with mounting local, national and regional compliance requirements by reducing manual and redundant processes and by speeding up analysis and reporting. Even more valuable is the way in which a pervasive GRC framework can significantly reduce the costs associated with risk incidents (as well as regulatory and compliance fines) while also contributing to more informed and more strategic decision making at the highest levels of an enterprise.

A pervasive program is imperative not just for managing GRC activities but also for linking those activities to broader brand and reputation management.

**Four Key Drivers**

In addition to the quantitative measures of GRC savings, what are the essential metrics by which organizations can gauge the necessity of implementing a pervasive GRC framework? To answer these questions, we break down the four elements (see table, below) that should be driving every organization's GRC cost-benefit analysis.

**The Qualitative and Quantitative Benefits of GRC**

| Qualitative Benefits of a GRC System | Quantitative Savings from a GRC System |
|---|---|
| 1. Embeds compliance requirements and helps a firm avoid regulatory fines. | 1. Rationalization of support and fees. |

| | |
|---|---|
| 2. Makes risk managers core to business management. | 2. Ensures that a firm is implementing controls that can be linked directly to a policy, compliance requirement or key risk. |
| 3. Considers top-line effects. | 3. Focuses assurance and testing activities on the controls linked to primary, high-rated risks. |
| 4. Institutionalizes knowledge and makes internal collaboration easy. | |

In a future article, we will explore the quantitative items on the right-hand side of the table. For now, however, let's focus on the GRC cost-benefit analysis from the perspective of qualitative benefits:

**1. The cost of bad GRC.**

In just about every industry, complex regulations are not only here to stay but are also going to increase. From SOX to Dodd-Frank to Basel III, many companies have struggled to keep pace with new compliance requirements and changes to existing standards. Ongoing regulatory changes have certainly impacted corporate budgets, while also making risk and compliance audits progressively difficult.

The rising cost of compliance is perhaps only outweighed by the even larger expenditures that accompany fines for non-compliance and regulatory failure. Examples of this sort abound. In the past year, JP Morgan, in response to a number of regulatory investigations, stepped up to the plate, leading by example by announcing it plans to spend an additional $4 billion to fix risk and compliance issues. Similarly, Oklahoma Gas and Electric, following a recent court settlement, announced that it would spend upwards of $1.5 billion to ensure compliance with new environmental rules.

By providing a framework that embeds compliance standards into company-wide systems and processes, a comprehensive and pervasive GRC platform can keep costs in check by ensuring compliance with changing industry regulations and mandates

**2. The visibility and importance of GRC related functions in today's enterprise.**

In recent years, a number of factors have contributed to the increased visibility of risk management's role in mitigating organizational losses. The financial crisis of 2008, heightened regulatory scrutiny, a rise in data breaches and operational failures in the face of natural disasters are just some of the risk scenarios that have left companies across a diverse number of industries feeling vulnerable and exposed. These changes to the risk landscape, however, have also necessitated a change in the risk posture of many organizations at the highest levels.

In an effort to be proactive, many companies are seeking to highlight their risk management and compliance efforts, making GRC-related jobs and processes more important and more visible than ever before. In this new risk reality, risk officers now have unprecedented access to the C-suite. By making risk management both a priority and an integral part of an organization, GRC technology expenditures can play a crucial role in demonstrating the serious commitment to managing risk that the current business environment demands.

**3. "Opportunistic" risk management can foster innovation and drive growth.**

Remaining competitive in today's business environment requires a continuous pursuit of new revenue streams and growth in existing revenue sources. This means that companies have to embrace moving outside of their comfort zones.

At its best, risk management not only allows organizations to mitigate risk but also to identify areas for growth and spur innovation. An integrated GRC system can help organizations achieve these goals in a number of ways.

First, a pervasive GRC program can help a company monitor risk levels and, over time, determine its risk appetite. Despite the fact that a sound risk appetite is absolutely essential for business growth, figuring out the level of risk that your firm is willing to accept is a significant challenge A dedicated GRC program can help a firm establish its optimal risk appetite by facilitating and driving collaboration among management with regard to defining clear risk tolerance levels and setting appropriate risk thresholds and limits.

Second, a GRC program can help aggregate data and insights needed to inspire innovative decision making and calculated risk taking. For example, the historical perspective offered by risk assessments and loss-event data provides organizations with the necessary intelligence to optimize resource allocations and to cultivate an approach to risk that aligns with their larger business goals

**4. The long-term value of a "system-oriented approach" to GRC.**

Maintaining rigid silos between business units is an ineffective approach to managing risk in an environment defined by connectivity and interdependence. Instead, what's required is a common understanding of risk that runs through every layer of an organization. The management of multiple GRC initiatives through a single system helps cultivate an appreciation for the interdependency of risk, and increases transparency and accountability through the implementation of controls that are shared across the organization.

Adopting a system-oriented approach also increases the effectiveness and long-term value of an organization's GRC program by creating a central repository of risk data that institutionalizes both internal firm data and external industry knowledge. By increasing the visibility of risks facing an organization, this central system of record lessens the negative impact of employee turnover and decreases the danger associated with critical business intelligence residing with just a handful of employees.

**Parting Thoughts**

GRC solutions are certainly far from one-size-fits-all. Different organizational goals will dictate different needs, and GRC is no exception. Today's global markets are hyper-competitive, defined as much by change as they are by the speed at which those changes occur.

By providing a comprehensive assessment of an organization's risk landscape, an integrated GRC platform can prove adaptable and agile, enabling a company to keep pace with shifting compliance standards and regulatory policies - as well as with evolving business goals.

As risk management professionals, we are constantly engaged in calculating and evaluating the potential upside and downside of a diverse number of internal and external risks. In this regard, risk management professionals are no strangers to cost-benefit analysis.

Of course, like any good attempt at calculation, determining your inputs is essential. The four key drivers highlighted in this article reveal the true value of GRC - not only in terms of decreasing losses but also with regard to helping organizations realize new opportunities.

There's little doubt that measuring the ROI of a GRC platform represents a formidable task. However, what remains clear is that in the context of a risk environment subject to constant change, and in a regulatory landscape that continues to evolve, the long-term costs of not having a company-wide, pervasive GRC program will far outweigh the investment required to implement and maintain one.

*Brenda Boultwood is the senior vice president of industry solutions at MetricStream. She is responsible for a portfolio of key industry verticals, including energy and utilities, federal agencies, strategic banking and financial services. She has had a rich career in risk management, and has held several key operating roles at some of the largest global organizations.*

*Most recently, prior to joining MetricStream, she served as senior vice president and chief risk officer at Constellation Energy. Prior to that, she served as global head of strategy, Alternative Investment Services, at J.P. Morgan Chase, where she developed the strategy for the company's hedge fund services, private equity fund services, leveraged loan services and global derivative services. During her tenure at J.P. Morgan Chase, Brenda also served as global head of strategic risk management for its Treasury Services group. Earlier in her career, at Bank One Corporation, she worked as the head of corporate market risk management and counterparty credit, and head of corporate operational risk management, before advancing to head of global risk management for the company's Global Treasury Services group. She has also been a board member of the Global Association of Risk Professionals (GARP), and currently serves on the board of the Committee of Chief Risk Officers (CCRO).*

Share: