

[ANNUAL CONFERENCE TOPIC]

A Strategic Framework for Governance, Risk, and Compliance

To address strategic issues, some organizations have developed initiatives referred to as GRC, which look across their risk and control functions holistically and seek to enhance their efficiency and effectiveness.

The business environment over the past few years has experienced an unprecedented series of issues, surprises, and negative events that have increased the focus on the adequacy of organizations' governance, risk, and control activities. Some of these events have caused many organizations to increase their budgets and staffing for their compliance functions. At the same time, other issues were prompting increases in internal audit and risk management functions. In many cases, these additional investments have been made at a tactical level within each of these control and risk functions without enough regard to what other, related risk and control functions were doing. The growth in these specific risk and control functions has led to concerns in many organizations about the total cost increases for these activities and about line business units being swamped with governance activities.

These concerns have led to the creation of initiatives now referred

to as integrated Governance, Risk, and Compliance (GRC) that seek to improve both the efficiency and effectiveness of an organization's risk and control functions. Many organizations are considering some type of GRC initiative, so we present a model and approach that may be useful to organizations dealing with these issues.

The Risk and Control Landscape

A primary driver of these initiatives was the Sarbanes-Oxley Act (SOX). In responding to the requirements of SOX, a number of organizations formed control functions to facilitate the actions needed to comply with the Act. Often, there was a corresponding increase in internal audit budgets to enable testing that was also required. This was occurring at the same time that many organizations were expanding globally and increasing their legal or compliance budgets to address requirements of the Foreign Corrupt Practices Act (FCPA). Further, some were also implementing or expanding risk management functions as that discipline was evolving. Because these investments or expansions usually were driven by specific issues, there was a tendency to deal with them individually

at a tactical level. Sometimes these investments were simply "bolted on" to existing activities.

When viewed from the perspective of the line business units, the increase in activities of these expanded risk and control functions has been challenging and has raised a number of concerns. Unnecessary duplication is one. There may appear to be duplicate activities or requests for information that don't seem coordinated between the risk and control functions. Business units will also express concerns that they believe they are dealing with multiple parties on the same topics.

From the organization's viewpoint, the growth in its risk and control functions has been increasing at an unsustainable pace. While organizations are very serious about these activities, the expense pressures today are forcing them to take hard looks at their total costs, including the costs for risk and control. Additionally, the level of concern being raised by some organizations' line business units has risen to the executive levels. Finally, as executive management and directors focus on understanding and addressing the organization's strategic risks, they may feel that

the increased activities in their risk and control functions have been too tactical and aren't helping them address strategic issues.

What Is GRC?

To address strategic issues, some organizations have developed initiatives referred to as GRC, which look across their risk and control functions holistically and seek to enhance their efficiency and effectiveness. These companies look to enhance efficiency by identifying and integrating certain processes and activities that are common across the GRC functions, such as risk assessments, which are typically performed by each of these functions. Effectiveness is also enhanced by better sharing of knowledge, data, and technologies. The organizations strive to build an environment where the GRC functions recognize that, while each has a unique role, they share certain common objectives and must work better together to achieve those common goals: for example, agreeing on the most significant risks facing the organization or compiling one consensus list of the most critical open issues across the GRC

units. As an additional benefit, the GRC initiative should also help ease the burden on the line businesses by better coordination and clarification of roles. For example, the GRC units may share their

planning schedules among themselves to avoid overlapping visits or work together to form combined teams to facilitate a single visit to a unit.

To help organizations better understand GRC, we offer a *Strategic Governance, Risk, and Compliance Framework*, which we developed when working with GRC practitioners and thought leaders. This framework makes it clear that all GRC functions share common goals, which ultimately are the creation and preservation of stakeholder value, a primary goal of enterprise risk management and strategic risk management. (For more information, see

May 2007.)

The functions also operate under a common governance umbrella, the organization's risk management policy as established by the board of directors. The framework recognizes the unique role of each function and demonstrates that GRC isn't an attempt to simply merge these functions into one. Effectiveness and efficiency are enhanced by leveraging common activities and processes "below the line" across these functions.

The Framework

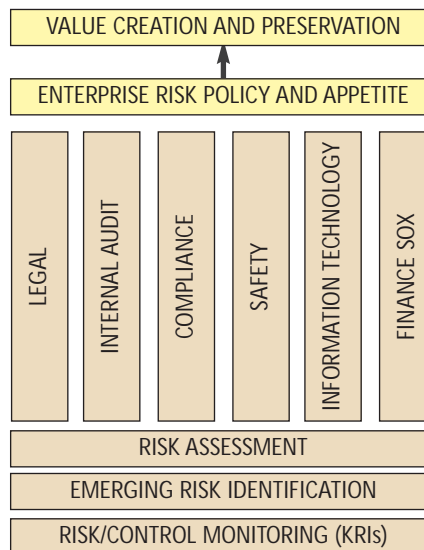
The *Strategic GRC Framework* begins with setting and articulat-

Strategic Governance, Risk, and Compliance Framework

Overall Policy and Risk Appetite Set by Board and Executive Management

Each Risk and Control Function Continues to Execute Its Unique Role as Part of a Fully Integrated Effort with a Common Goal to Manage the Organization's Risks

Functions Identify and Leverage Common Processes, Technologies, and Knowledge



Policy establishes:

- Role of Each Function
- Common Goal of Managing the Organization's Risks
- Risk Framework
- Expectation of Working Relationships and Knowledge Sharing

© Copyright 2009 by Mark L. Frigo and Richard J. Anderson

Mark L. Frigo, "When Strategy and ERM Meet," *Strategic Finance*, January 2008, and Mark Beasley and Mark L. Frigo, "Strategic Risk Management: Creating and Protecting Value," *Strategic Finance*,

ing the organization's "Enterprise Risk Policy and Appetite." This is a board-level policy that establishes the strategic risk policies and related risk appetite of the organi-

continued on page 61

Strategic Management

continued from page 22

zation. The policy sets the common overall goals of value creation and protection as well as the expectations for the working relationships among the GRC functions. These common expectations can include items such as:

- ◆ An overall focus on strategic risks to shareholder value,
- ◆ Maintaining an enterprise-wide perspective,
- ◆ The sharing of information and knowledge,
- ◆ Common development and investment in technology and tools, and
- ◆ An enterprise-wide risk framework and language.

The policy should also articulate and clarify the role of each GRC function. The development of this section of the policy is an opportunity to clarify and then communicate the primary roles and activities of each function. This may be very useful in building a better understanding of these roles and their relationship to each other across the organization's line business units.

Pitfalls

It's very important to clarify at the start of any GRC initiative what the objectives of the initiative are and aren't. As noted, the *Strategic GRC Framework* acknowledges the unique role of each risk and control function. It's an exercise in leverage and clarity, not an exercise in corporate reorganization. That objective needs to be clear up front because if the GRC initiative is perceived as just an organizational restructuring, turf battles

will probably kill it. Also, while there's a need to clarify the various roles of the GRC functions, the initiative isn't meant to be an open door to completely rethinking the traditional core roles of these functions.

Finally, not all organizations have experienced the dynamics that have given rise to GRC. Some are just now thinking about implementing activities such as a risk management function. The *Strategic GRC Framework* can be a useful tool in this situation. It can serve as a model when building or expanding risk and control functions so that the integration of common processes can be built into the design up front, avoiding the need to reengineer them later.

Reaping the Benefits

The current environment of cost control and reduction probably means some form of GRC is here or coming for most organizations. Beyond the cost issues, a properly conducted GRC initiative, built off the *Strategic GRC Framework*, offers companies an opportunity to increase the overall effectiveness of their investment in their GRC functions. The framework also enables the GRC functions to participate in the initiative without hidden reorganization agendas. Finally, executive management and directors should have a better and clearer understanding of the roles, relationships, and operations of their GRC units. **SF**

Mark L. Frigo, Ph.D., CMA, CPA, is director of The Center for Strategy, Execution and Valuation and Ledger & Quill Alumni Foundation Distinguished Professor of Strategy

and Leadership in the Kellstadt Graduate School of Business at DePaul University in Chicago. An expert in strategic risk management, he is leading the Strategic Risk Management Lab at DePaul. Mark is co-developer of the Return Driven Strategy framework (www.returndriven.com) with Joel Litman. You can reach Mark at mfrigo@depaul.edu.

Richard J. (Dick) Anderson is Clinical Professor of Risk Management in The Center for Strategy, Execution and Valuation and Strategic Risk Management Lab at DePaul University and a retired partner of PricewaterhouseCoopers LLP. At PwC, he was a regional leader in the Financial Services Advisory practice, consulting with major financial services organizations on internal auditing practices, risk management, and audit committee activities. You can reach Dick at danderson012@hotmail.com.

Mark L. Frigo is a speaker at IMA's Annual Conference, June 6-10, 2009, in Denver, Colo. For information, visit www.imaconference.org.
