

# Positioning GRC and ERM

*Placing these puzzle pieces together to improve performance*

By Mary Peter

Getting GRC and ERM to work together is challenging for those who have been involved with governance, risk management, and compliance during their entire careers. The pressure from boards, stakeholders, rating analysts, regulatory agencies, and government has created a swell of solutions that further complicate how an organization chooses to implement or integrate a process to better address risk. As with any complicated puzzle, it helps to step back and look at the big picture first, sort out the colors and segments, then put the pieces together in a strategic way.

GRC is comprised of *governance*, which is the process by which the board sets the objectives for an organization and oversees progress toward those objectives; *risk management*, which means different things to different organizations, but is typically seen as risk mitigation, IT risk management, risk transfer; and *compliance* which addresses both government and industry-specific compliance, such as banking regulation, NAIC Risk Focused Exams in insurance, Sarbanes-Oxley Act (SOX) for public companies, and the Health Insurance Portability Accountability Act (HIPAA). Often these risks are addressed from a reactive perspective, and companies are not able to focus on the specific goals and objectives of the organization. Further, by the time risks have entered the GRC space in most companies, an informal decision has been made that they qualify as risks the company intends to mitigate. This leaves all opportunity risks off the table for discussion.

ERM (*enterprise risk management*)

takes a broader view of risk management and is defined by the Risk and Insurance Management Society, Inc. (RIMS) as “A strategic business discipline that supports the achievement of an organization’s objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio.” ERM looks at risk management prospectively in a broad, more strategic, and purposeful manner.

Both GRC and ERM are high-level initiatives that are driven by the board of directors and executive management to reduce risk, optimize performance, increase profitability, and provide transparency. In most cases today, GRC is the umbrella, with ERM being “represented” in the risk-management section of GRC.

The puzzle pieces of GRC and ERM are applied in this manner:



In this view, ERM is the smaller puzzle piece and part of GRC, and therefore may not receive the optimum level of attention to address an emerging risk or an organizational opportunity. Lessons learned from the global economic crises and the recent environmental disaster has brought scrutiny on the risk management practices of individual companies, industries, economies, and governments. The practice of risk management in a siloed environment does not contain the appropriate account-

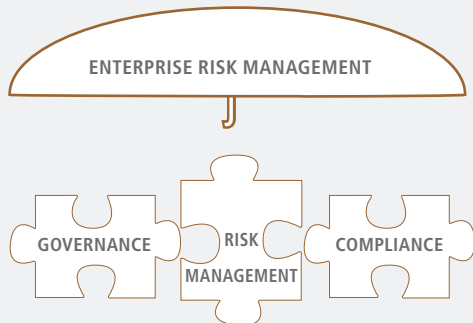
ability and connection to an organization’s goals and strategic objectives. Incorporating ERM into the GRC model may actually perpetuate the siloed approaches to risk management which operates at the risk and control levels within the detailed areas of the organization.

With a GRC centric approach, the tendency is to look at invested capital for an initiative and focus on tangible assets. Consider the risk of a failure of equipment, creating an oil spill in public waters. An assessment of this risk would typically involve a look at fines, penalties, clean-up costs, and profit loss. The missing elements in this view are the intangible assets or those which are difficult to quantify. If you were to add the intangibles into the equation—for example, the future costs impacted—to include legal fees, regulatory investigation, government involvement, public relations, media cost, and reputation risk, the true capital at risk equation would be invested capital plus the intangibles. This results in adding the prospective costs of capital for the entire risk, across multiple departments and how that fits into the company’s risk appetite. This capital at risk closely relates to sustainability of the organization and is a more effective enterprise-wide approach to managing the company’s assets. In the example of the environmental risks due to an oil spill, the costs of the intangible assets go beyond the invested capital. The impact of the spill not only includes the assets of the company responsible, but their vendors, the surrounding partners, communities, and the overall environmental impact. The true cost of this loss will take years



to fully understand and recover from.

Now consider for a moment that this type of risk instead becomes a key part of the ERM process, and risk management becomes the vehicle as to how an organization decides to respond to its risks. In this view, ERM is placed above GRC and the puzzle pieces fit differently. It looks like this:



In this configuration, the puzzle piece of ERM is larger in scope and placed as an umbrella over GRC.

Historically, risk management has been or can be viewed as a way to mitigate or transfer risk by using controls or insurance. In most organizations, risk management is not fully utilized to look at risks prospectively or across the entire organization, considering the interdependency of risks and their outcome to the whole organization. ERM is an archway for the company to take a holistic approach for the company's risk management and bridges the departmental risk-management tools and processes. By clearly defining ERM as your framework and then bring-

ing the *governance, risk management, and compliance (GRC)* together, the company can increase the strategic vision and direction to meet its goals. When an organization looks at their enterprise risks, it becomes clearer which risks are the most significant in terms of impact or probability to the entire organization. These risks are then prioritized; appropriate risk response plans are put into place and communicated across the organization.

When an enterprise risk-management view is structured as the over-reaching umbrella initiative, risks are seen through a bigger lens. This view includes looking at the risk and its response options and seeing if they align or conflict with the mission, vision, goals, and objectives of the organization, as well as their defined risk appetite. Obtaining information from cross-functional teams provides executive management and the board with key metrics and prospective views for improved decision making.

ERM is also an internal process that elevates the most pressing and opportunistic risk-taking initiatives to the highest level for attention. Some companies have found that when they implement ERM within their GRC program the puzzle pieces do not seem to fit. By stepping back and looking at how the pieces have come together for other companies who have defined an ERM framework first and fitting current GRC tools into their ERM program, the puzzle comes together in a unique fashion for their organization's strategic plan. This clearer picture effectively supports the vision, mission, sustainability, and performance of the organization. ■

Mary Peter is Director of Enterprise Risk Management at Eide Bailly LLP and leader of their ERM consulting services, with over 20 years experience in risk management and insurance. She is a member of the ISO 31000 Risk Management Standard - US Technical Advisory Committee, and its subcommittee currently writing an implementation guide for ISO 31000 for the United States. She is a member of Risk Insurance Management Society (RIMS), and participates on a RIMS crosswalk committee



comparing worldwide risk management standards such as COSO, ISO 31000, BS 3110, and FERMA. Mary is co-chair of an ERM Roundtable that brings risk management and audit disciplines together in the Minneapolis/St. Paul area, and is a frequent speaker on ERM.

This article was produced by Eide Bailly LLP with the understanding that the information contained does not constitute legal, accounting or other professional advice. It is not intended to be responsive to any individual situation or concerns as the contents of the publication are intended for general informational purposes only. Readers are urged not to act upon the information contained in this publication without first consulting competent legal, accounting or other professional advice regarding implications of a particular factual situation. Questions and information for publication can be submitted to your Eide Bailly representative or author of the article. Copyright 2010.



CPAs & BUSINESS ADVISORS