CFO

Risk & Compliance | August 07, 2012 | CFO.com | US

Managing Risks Must Include Taking Them

Enterprise risk management and governance, risk, and compliance are not interchangeable. Why? The reasons lie at the core of the practice of risk management.

John Bugalla, Kristina Narvaez

Baseball great Yogi Berra once said: "If you come to a fork in the road, take it." For the practitioners in the art and science of risk management, the fork in the road is at hand. One directional sign says ERM, while the other says GRC. ERM is the acronym for enterprise risk management and GRC is the acronym for governance, risk, and compliance.

For CFOs, who often oversee internal audit and risk management, the issue should be about where each road will take them — and about the quality of the ride.

Some argue that it does not matter which road is taken, because they both end up in the same place. For them ERM and GRC are interchangeable. Yet another group of practitioners debates the question of primacy of either ERM or GRC — or which one is the umbrella over the other.

The reason ERM and GRC are not interchangeable lies at the core of the practice of risk management — what it was, what it is, and more importantly, what it will be. The outcome of this dilemma is significant beyond corporate practitioners. Investors in publicly traded companies, millions of people with 401(k) accounts, and the additional millions with pensions should have an interest.

Background

Risk management is rooted in the concepts of preserve, protect, and comply. Preserve assets, protect people, and comply with laws and regulations. Techniques employed to achieve these goals are a combination of risk transfer, commodity and financial hedging, safety and loss control programs, and legal contracts. This is a traditional approach to risk management.

About 20 years ago, academics and practitioners started to view risk not only from a downside perspective, but more like a coin with two sides—up and down. Traditional techniques are still employed, but the result of this thinking is that risk is viewed from a much wider lens with a greater depth of field. Risks are consolidated across the enterprise (hence the name enterprise risk management) and seen as a dynamic overall portfolio.

It is worth noting that during the time risk management was evolving, events were taking place that also had a significant impact on the practice of risk management. The dot.com collapse, financial scandals such as Enron, backdating of stock options, the financial crisis of 2008–10, the BP oil spill, and other significant events brought a new era of attention from regulators.

New regulations are especially apparent in the area of financial disclosure and reporting with the notable examples of Sarbanes-Oxley, SEC Amended Rule 33-9089, and Dodd-Frank.

The Fork in the Road

Risk management continued to evolve, but it has diverged into two schools of thought that are now evident, more by practice than by theory. Sarbanes-Oxley spawned GRC, which is driven by compliance and audit.
Supporting the GRC process is a host of technology platforms. The technology organizes and highlights governance structure and compliance risks coupled with documentation and reporting requirements.

The primary goal is assuring the integrity of financial statements and compliance with myriad laws and regulations. Some detractors of GRC suggest that the "C" (compliance) carries greater weight and focus than the "G" (governance), which in turn carries greater weight than the "R" (risk).

Conversely, ERM is a risk management process meant to encompass all risks and opportunities across the entire enterprise—including the GRC components. One ERM best practice is to embed the process into strategic planning. The reasoning is that ERM should support the plan that at its core is a strategy for growing the business.

The very nature of a strategic plan, however, is a multiyear time frame that is usually crafted around several plausible operating scenarios. Supporting organizational growth strategies is one goal, with the other traditional goal being to mitigate and lessen the impact of adverse events that could occur during the plan.

One example is a company that has determined that an acquisition opportunity should be pursued. Any acquisition can produce a range of outcomes for the acquirer. The ERM process is a tool for decision makers that enables them to consider and measure the steps to achieve the upside gain as well as plan or take the steps to manage or control adverse events that could destroy anticipated value. GRC, however, does not consider the upside of risk-taking activities, but focuses on controlling activities.

Viewing governance, risk, and compliance holistically can help streamline these important processes. Done right, an integrated GRC program incorporates a technology infrastructure that highlights critical issues driving attention toward such issues as transparency and accountability.

Compliance: Just Part of the Picture

Being in compliance with rules and regulations does not necessarily translate to best practices in risk management. The

financial crisis and the failed institutions associated with it have proved that being in compliance does not necessarily prevent the destruction of shareholder value, savings in 401(k) accounts, or pension valuations.

An effective ERM program, on the other hand, which addresses a wider spectrum of risks, goes beyond pure risk mitigation and should improve the quality of decision-making. When ERM is embedded into the strategic-planning process, it adds support for growth strategies of the business that can create value. After all, how can business exist if it does not take risks?

It should also be noted that for either GRC or ERM to meet the expectations of practitioners, executive management and the board need to establish and show their support to the rest of the organization.

If risk management is divided into a series of software modules and fragmented into the very silos meant to be broken down,

a great deal of time and money will have been wasted.

John Bugalla is a principal with ermINSIGHTS and Kristina Narvaez is president and CEO of ERM Strategies LLC.