There has been so much written about the topic of Enterprise Risk Management (ERM), it is tough to know where to start when addressing the topic. Our webinar on the topic focused on “The Role of ERM in your GRC program.” Of course, that assumes that your company has an active and efficient GRC program. Step one to integrating the two is evaluating your ERM processes to determine how to integrate and synergize activities to meet the requirements of both programs.

Stepping back for a minute, we know that an ERM program can be deployed in a variety of ways and can take on various meanings within organizations. With that in mind, a solid ERM program must embody a culture of risk awareness and risk identification. In essence, ERM is meant to empower business managers to make smarter decisions that maximize value, reduce costs and balance risk and returns. This can often require a culture shift or mindset change within an organization. Growing pains can be difficult and time consuming.
When you hear about ERM, you often hear that companies must be able to break down the silos and political barriers that exist between risk ownership. We’ve built our corporations through the development of critical processes owned by technical experts with the appropriate skill set to manage risks imbedded in that portion of the business. Traditionally, our organizations may have managed risks as follows:

- Strategic risk – senior executive team, CEO and board
- Financial risks – accounting department and CFO
- Treasury risk – finance and treasury personnel
- Credit Risk – credit managers
- Insurance Risk – insurance area
- Legal risk – lawyers
- Contract risk – lawyers and procurement professionals
- Compliance risk – regulatory areas or specific operational areas such as environmental health and safety
- Operational Risk – various operational areas
- Oversight and governance – Board of Directors

Of course, this is not meant to be an all-inclusive list but I think you get the idea.

Then the concept of ERM came out and companies were told they needed to develop a holistic approach to managing all of these risks. It would have been interesting to have an intercom in that first Board meeting of a traditional company when this concept was brought forth. Can you imagine the discussion?

“What do you mean? Why should anyone outside the CEO and Board understand strategic risk? Only lawyers can really understand legal and contract risk! Who better understands regulatory risk then our professionals who deal with the regulators on a day to day basis?”

There were probably quite a few other questions and explanations brought forth. But eventually, boards understood the reason for the concept. Then came the difficulty of obtaining buy-in throughout the company. Political barriers had to come down and required professionals (who may have previously managed an entire process) to work with other areas to ensure all appropriate risks were covered. Although professionals understood the dictates of their management to work through an ERM concept, the actual execution entailed many barriers and difficulties. All of a sudden, information needed to be available to various individuals. Some of that information may have been confidential or considered proprietary. How was the organization going to ensure that it crossed all T’s and dotted all I’s?

Now we are many years into the concept of ERM and some companies have created elaborate risk universes, tracking processes and risk reporting methods. COSO created the COSO ERM framework which added concepts to the original COSO framework to help further identify areas that should be incorporated into an ERM process. We have to ask the question, have we accomplished the true intent of what ERM was trying to address? Or are our processes just a massive effort in risk identification, risk ranking, risk reporting and risk analysis.

The concepts of ERM have significantly added to the control structure of organizations. It has helped to place a framework around all of those risk processes that were previously siloed within an organization. boards and management are now more aware of various risks that may impact their strategy and long-term development. Professionals have a better understanding of how risks may impact their everyday jobs. Time is often allocated within strategy settings and board meetings to address the topic of ERM. All of these things have advanced the cause of appropriate risk evaluation and analysis that so many of our shareholders, creditors and regulators have asked for.

However, it goes without saying that incidents continue to occur within our business environments. And possibly it is naïve to think that we can completely eliminate the many corporate failures or miss-steps that have happened over the years. It also begs the question of whether the highly publicized downfalls are an outcome of a company who has actively employed and executed appropriate control structures and ERM processes and now issues are identified and brought to the attention of the investing public. Or, are we just more aware of issues that have been occurring for a long time because there are more regulations, legislations and rules that guide corporate behavior? Think about many of the recent corporate scandals that have occurred. Many of them are things that date back several years. ERM has been around for more than a decade yet many of these issues are now just coming to light. Is it because ERM takes a long time to appropriately evolve, or is it because there are enhanced legislation and monitoring by the regulatory bodies relating to some of the issues that have occurred?

Regardless of your perception on this issue, the concept of ERM can be a very good thing for companies and a very valued oriented approach to identifying, managing and monitoring risk on an ongoing basis. Enterprise Risk Management creates an enterprise-wide view of risks. This view increases probability that organizational objectives are more likely to be achieved. It creates value preservation and enhancement. However, for ERM to be successful, it must be driven from the top down. This means active involvement from the Board and the senior executives. ERM is meant to be value adding and should be integrated within strategic planning. There can be no sacred cows or off-limit areas when it comes to ERM. All processes and risks are open to
Reflecting on these assumptions, it is not uncommon to hear from executives:

- “We know the concepts…”
- “We know the theory…”
- “We know the benefits…”
- “Our organization manages risk…”
- “We have an official ERM program…”
- “We take risk seriously…”
- “Our board understands ERM…”
- “We frequently report to our board on risks”

Many corporate individuals will say they can positively affirm to the preceding questions. If that is really true, then where is the gap between formal programs and true execution? Studies tend to show that companies still struggle. A recent study indicated that companies that suffered the greatest losses indicate there is little to no alignment, coordination, or leverage of risk assessments. The study also showed organizations lack access to current information required for senior management to respond quickly to emerging problems. As a result, the bad things continue to happen because we may be concentrating on form over substance when it comes to our ERM programs.

So now we get to the reason why it is important to attempt to converge ERM processes with GRC processes. Although regulatory and business risks vary in scope and complexity, the process for identifying, measuring, monitoring and managing them can be very similar. Convergence of the two can help companies meet the increasing burden from regulatory compliance requirement. It can synergize risk management efforts and gain tangible benefits across the organization. Convergence will allow business managers to spend less time on assessments. Managers can spend more time on proactively managing risk and processes to meet company objectives.

But to ensure effective convergence, management must affirm that their current processes are effectively developed and employ the proper substance rather than just form. They must be able to look at all of those intricate risk assessments, risk maps, risk evaluations and scenario analysis and be able to determine whether they have been adequately performed with the proper resources and assigned individuals and without bias to organizational responsibility. Management must be able to reconcile the risk assessments performed by Internal Audit, Legal, Compliance, Regulatory, the ERM group and any others to ensure they are appropriately aligned and have all relevant concepts. Failure to recognize the overlap of activities may hinder ability to effectively assess enterprise-wide risk and the adequacy of internal control systems. One caution: be careful of the political trap and territorial issues.

Management should set out clear accountabilities and responsibilities in relation to risk management and compliance. This will assist in managing inter-dependencies of risks. Remember, no one group is responsible for all risk. It is imperative to ensure all professionals work together. Think, are there instances in your organization where some of the following may be assumed?

- “Internal Audit owns Sarbanes-Oxley”
- “The Legal department is the only area that can handle contractual risk”
- “The insurance group can manage all insurable activities without interaction from other groups”
- “The compliance function is solely responsible for all new regulations and laws”

Whether it is one of these scenarios or something different, management must work through the perceptive barriers to ensure there is a holistic view of ERM and GRC. To enforce this concept, ERM and GRC must be more than just an initiative; management must fully support it and establish clear accountabilities and concepts. They should establish a strategic vision and implementation plan that ties to corporate strategies. You may want to consider a phased approach to implementation. Sometimes the big bang approach isn’t the best alternative.

Another important aspect is to focus on a risk awareness culture. Don’t just say, do! ERM should converge and harmonize processes. The company should maintain a common risk rating system, agree on key risk indicators and eliminate duplicate and redundant assessments. Another important concept is to identify the role technology will play. There are many software providers that have tools to help facilitate both ERM and GRC. However, ensure you recognize that technology is a tool and an enabler; it is not the entirety of the program.

Last, it is important to right-size ERM to your company. Your ERM program must be flexible to respond to change. It must be tailored to organizations corporate strategies, business activities and external environment. The concept must be embedded into the organization and have an appropriate foundation for execution. Develop a comprehensive and integrated suite of applications. Applications should address: financial controls management, operational risk management, compliance risk, IT risk and compliance, Internal Audit. An overall integrated approach to managing and monitoring your ERM program will facilitate convergence with GRC and assist in providing your company an integrated approach to data knowledge.