10 Easy Steps to Implement Enterprise Risk Management

Carol Fox | *November 14, 2012*

At RIMS, we define enterprise risk management (ERM) as a discipline, not in the sense of punishment, but as the mastery and continued maturation of risk competencies. Essentially, ERM is all about building risk management capabilities throughout the organization.

As risk professionals, we often focus on ERM as an end to itself rather than a means to support the organization's objectives. But to be useful, that is exactly what it must center around: providing value to the company.

Alas, there is no magic bullet to implement a program that will hit that target. But there are some key guidelines you can follow. With that in mind, the following 10 simple steps may help guide you as you begin planning your journey.

1. Define what value your organization will gain from ERM

Because it is so difficult to demonstrate ERM value through traditional investment metrics (return on investment, return on equity, return on assets, or risk-adjusted return on capital), many companies make the business case. This looks at ERM in four categories: shareholder value, risk mitigation, process consolidation and silo elimination.

While these are worthy goals, they can be difficult not only to measure but to articulate to management and the board. Since leadership is always focused on value creation, the link between ERM and the organization's strategy is often weak at best.

So how does ERM actually contribute to the organization's value? How can that be demonstrated and measured in terms that are

meaningful?

You first have to discover what value your organization is trying to create, as well as protect. Is it simply increased share price? Or is it reducing volatility to enable a more efficient use of capital? Or perhaps, for non-profits, is it delivering more services to a broader constituency?

Whether value is expressed as market share, profit, service provision, donor levels, social impact or some other benefit, how do the enterprise risk management competencies advance the organization's mission and related objectives? In other words, what business need will be met through a structured ERM approach?

2. Research and understand different standards and frameworks

Advocates of certain risk management standards and frameworks may encourage you to believe that there is one, and only one, "right" way to define and manage risk. If you operate in a regulated environment, you indeed may need to comply with specific risk management standards. But risk management practices tend to be universal and evolve over time, whereas standards (and regulations, for that matter) may not keep up with more current, innovative practices.

Even so, learning about each of the major standards can generate ideas. A 2011 RIMS executive report, "An Overview of Widely Used Risk Management Standards and Guidelines," analyzed six frameworks, and nearly all were found to be similar in certain ways. For example, each requires, among other aspects, the adoption of an enterprise approach with executive-level sponsorship; structured process steps, oversight and reporting of the identified risks; a risk appetite definition with acceptable tolerance boundaries; and monitored treatment plans.

Although we uncovered a number of common elements in our research, certain success factors were either missing or underdeveloped, most notably root-cause analysis and risk appetite management. Moreover, we found that 44% of North American risk practitioners choose to adapt their practices from a number of standards rather than adopt any one standard. Learning as much as you can will give you a solid foundation to decide what elements are the most vital to *your* ERM initiative.

3. Inventory what your organization is already doing

Many organizations already have controls in place for widely understood risks, such as business disruption, environmental liability or worker injuries. It is likely that the individuals responsible for these controls also conduct risk assessments. While this is not enterprise risk management, it is a start. And understanding what your organization is already doing allows you to leverage existing practices within a broader ERM environment.

Additionally, having a common, collective understanding concerning which risks should be accepted, avoided, transferred (or shared), mitigated or exploited can reduce organizational dissonance about what is acceptable to the organization's stated objectives.

4. Seek support and help

Implementing an enterprise risk management program is not the time to go solo. Many parts of the organization have a legitimate stake in the discussion, and they can become either powerful allies or forceful detractors. The "power of one" comes into play in recruiting those who can make a positive difference in your implementation.

Your most important advocate should be an executive sponsor—ideally more than one. Once your sponsors are on board, determine who best understands the risks your organization faces. Many successful implementers have formed a working committee of internal stakeholders, such as operations, sales, accounting, legal and internal audit. If you include the leaders responsible for management controls in a working committee, it usually accelerates collaboration.

Mostly, however, you should seek out people who are knowledgeable about your organization and able to influence others, which means the cast may vary depending upon the scope of operations. If your organization's mission is innovation, for example, include leaders from research and development. Or, if your organization focuses on education, include faculty leaders.

You may also want to consider external sources of support, such as insurance brokers, external auditors or consultants. But heed this word of caution when engaging external supporters: be sure to clearly communicate the specific role you want them to play. Sometimes, this may require a strong nondisclosure agreement.

5. Keep it simple

Focus on the basics. Once you have established why you are implementing ERM, work to de-mystify the process. Be able to distill your messages down to two-minute sound bites that explain, in plain English, how ERM is different from previous approaches. Refrain from using jargon; choose terms that are already understood in the organization. In the same vein, simplify process graphics to illustrate the steps the team will be taking.

Remember to keep the message focused on the organization's objectives rather than on the risk management process itself. To the end user, the ERM program mandate is less important than gaining value by making better-informed decisions about risk. While a formal training program may be characteristic of a mature program, simple process training, using available tools and templates, is quite appropriate when first getting started.

6. Start small

What should be the scope of an ERM implementation? A number of successful implementers have begun by focusing on a specific business area or single goal. The state of Washington's strategic goal is to improve the health and safety for all citizens, for example, so its ERM goal became fostering ERM implementation in all of its 165 state agencies.

While this scope may seem daunting at first, nine specific and achievable objectives—including assigning risk management to a specific employee within each agency—were agreed upon over a multi-year period. Parameters were set for success, and the scope of activities was limited in a manageable way. By initially targeting implementation in a controlled way and monitoring progress against a single goal, Washington achieved a higher overall commitment. And now the state has something it can build on.

7. Go for the quick wins

Don't try to cover every possible risk. Start with those that matter most for the success of your organization's strategic objectives. By identifying and analyzing the risks that may have a material impact on the ability to execute strategy, the odds of creating value quickly are much higher. If you prioritize by risk criteria—severity, importance or speed to onset—action plans can be executed immediately and revisited to validate the chosen responses.

Understanding which risk criteria are important to leadership creates an opportunity for frank discussions about just how much risk the organization wishes to pursue, both for specific objectives and in the aggregate. These leadership discussions tend to reveal where the organization may be culturally when it comes to risk-taking or risk aversion. Overall, this exercise can go a long way towards establishing a barometer of the organization's risk appetite.

8. Delegate "fixes" to risk owners

Who will do something about the risks? The obvious answer is whoever is accountable for managing the business functions most closely associated with those material risks. For example, a chief information officer may be accountable for managing risks associated with potential data breaches.

Not all risks can be neatly compartmentalized, however. Risks such as unauthorized social media releases may not find a "natural" owner, but a specific individual still needs to be named. There always should be one identified owner held accountable for the risk management plan decisions and execution. This person will likely need to rely on others to make the plan work and manage interconnected risks, but naming an individual risk "owner" will help move the chosen response plan to action.

9. Report on progress

Progress reports highlight the difference that enterprise risk management makes in your organization and should be reported in at least two ways: by material risk and by ERM program progression. The risk owners should be reporting in their normal business updates on key issues, such as the material risk outcome target, specific activities that have taken place since the last report, challenges in executing the risk plan, and a trend assessment in the risk profile against the targeted outcome. Periodic reports to senior management on ERM program progression might include progress related to milestones for specific ERM objectives.

In Washington state, one of those milestones is the percentage of agencies that assigned risk management responsibilities to a specific employee over defined time periods. One result shown in a 2011 ERM progress report was self evident: a liability reserve reduction of $600 million. And an intangible result was that the organization improved its overall risk management capabilities and competencies throughout its 165 agencies.

10. Develop your "soft skills"

How do you "sell" ERM within the organization? First of all, understand the dynamics of your internal market. People "buy" what they perceive to be of worthwhile to them and to their performance objectives. The question you need to be prepared to answer is "what benefit will they gain if they implement enterprise risk management practices?"

There is power in positive persuasion. Focus on the expected positive outcomes for the individuals you want to engage rather than trying to convince leadership that "we have to do this to comply with our ERM policy." Above all, you need to be an excellent communicator with a specific value message: "Enterprise risk management is a discipline that protects—and creates—value for the organization. By implementing ERM, you personally will be able to deliver results with both tangible and intangible benefits." n

---

Special acknowledgment to Richard W. Sarnie, vice president of risk management at the Atlantic and Pacific Tea Company, Inc, who, along with Fox, gave the presentation on which this article is based at the 2012 RIMS Annual Conference & Exhibition in Philadelphia.

***Carol Fox**, ARM, is the former vice president of strategic initiatives at RIMS.*

Topics
Enterprise Risk Management

Related Articles