Enterprise Risk Management: The Final Frontier

By Melanie Lockwood Herman

Executive Director

Resource Type: Articles

Topic: Enterprise Risk Management

It's hard not to notice the growing use of the term "Enterprise Risk Management" among risk professionals. Yet there seems to be little agreement about what that combination of three words really means, and perhaps more importantly, whether the addition of "enterprise" to the more familiar term "risk management" makes a bit of difference.

According to author Michael Power (*Organized Uncertainty: Designing a World of Risk Management*, Oxford University Press, 2007), ERM "… signifies any aspiration for a form of risk management practice which is all-encompassing in scope, business-focused, and is suggestive of a bird's eye view of organizational life."

In the introduction to their book, "Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives," chapter authors and book editors John Fraser and Betty J. Simkins write that "Enterprise risk management (ERM) can be viewed as a natural evolution of the process of risk management."

A study of how ERM has evolved describes the two predominant views of enterprise risk and the corresponding style of ERM program:

- Organizations that adopt an *enterprise-wide* view of risk (i.e., want to understand each risk across all departments or functions) tend to develop ERM programs that "take a more operational / financial view, and manage risks through quantitative control."

*[Author's Note: I owe a debt of gratitude to Diana Del Bel Belluz of Risk Wise Inc., for her thoughtful review and helpful additions to the draft of this article. Sign up for Diana's terrific newsletter, the Risk Management Made Simply Advisory at www.riskwise.ca/advisory-a-tips.html.*Organizations that adopt an *enterprise-level* view of risk (i.e., want to understand risks to the achievement of strategic goals and objectives and the long-term sustainability of the organization) tend to develop ERM programs that "take a mainly strategic view of risk, and manage it in a qualitative way."]

The concept of ERM is more than a new term or a new label for an old practice; it represents the potential to look at risk practice differently. This is especially relevant and important in nonprofit organizations, where risk management programs are often in dire need of modernization.

Five Weaknesses in Nonprofit Risk Practice

During nearly 20 years of consulting work with both brand name and lesser-known nonprofit organizations, I've observed five common weaknesses in the risk management function. These fault lines include:

1. **Failure to define "risk" before talking about what to do in a world of continuing uncertainty** – Many years ago my colleague Diana Del Bel Belluz introduced me to the concept of a bow tie as a shape to help illustrate how people in organizations see and understand the term ¥risk' differently. At the center knot is the *possibility of an action or event that threatens to substantially impair or advance your mission or objectives*. The future "action" or "event" is a risk. For every risk, however, there are always underlying circumstances or conditions that give rise to or influence the timing, magnitude or other aspects of the risk event. These underlying conditions might be listed to the left side of the bow tie, along one of its broad edges. But there are also consequences□usually both negative and positive□when risks materialize. These could be listed to the right of the center knot, thereby giving shape to the bow tie. Unfortunately, when a group convenes to talk about risk, they often skip the first step: defining the term. As a result, a typical list of nonprofit risks includes risk events as well as underlying conditions and consequences.
2. **Misconception that risk management's focus is to eliminate or avoid as much risk as possible** – Countless nonprofit board and staff leaders have told me of their efforts to eliminate risk in order to pave a clear path to mission success. This thinking is flawed because risk and reward are inextricably linked. We take risks in nonprofits in order to create value for the communities we serve. In every decision or strategy for which the outcome is uncertain, there is risk. Zero risk exposure means no opportunity for creating value. Whichever goals or strategy a nonprofit embraces, there will be a set of opportunities and a set of risks associated with it. The goal of enterprise risk management is to help understand the particular risks that are associated with each strategic option in order to make informed and deliberate decisions about which objectives and strategies to pursue and the corresponding risks that must be accepted and managed. In my experience, high performing nonprofits spend more time evaluating risk-taking opportunities, than eliminating or avoiding risk altogether.
3. **Excessive focus on scoring risks and finding a "tool" to automate risk management** – Listing downside risks in a spreadsheet or table and assigning scores for risk likelihood/probability or impact/ severity is a well-known practice within risk management. Yet the Center's experience is that this approach, sometimes referred to as a "risk register," does not inspire timely action in the face of uncertainty. Nonprofit leaders are motivated by many things, including the potential to serve a growing client base, meet donor expectations or demands, avoid legal liability and more. I've yet to meet a leader motivated by an opinion-based score in a risk register. An associated challenge with risk registers is the fact that once tabulated, scores seem somewhat scientific. But whether they are scribbled on a napkin or recorded in a risk register, they are generally arbitrary guesses about the likelihood and potential value (cost or benefit) of a future action or event. In my experience, risk management is really about hard conversations that enable leadership teams to make the best possible decisions in the face of uncertainty□ not finding or using the right spreadsheet, software or system.
4. **Conclusion that risk is harmful, or potentially harmful to a nonprofit mission** – Over the years I've written and spoken about risk's "bad rap." When the word "risk" comes up in conversation, it's not unusual to see a bead of sweat or a frown, and hear a sigh of frustration. Lawsuits, the admission of liability, the imposition of liability and the arrival of lawyers are the four horsemen of the risk apocalypse. Yet no nonprofit takes risk in order to suffer a loss. Risks are taken to advance, not erode a charitable mission. Therefore it is inaccurate to paint risk with the broad brush of harm or despair, or to limit risk management to a discipline about what can go wrong. Furthermore, when a positive development occurs, there may be negative consequences that require attention, and when a downside risk materializes, there may be unexpected positive results as well. Risk is far more nuanced that we often recognize.
5. **Perspective that a key to managing risk is assigning risk "owners"** – Nonprofits that turn to a "risk register" or spreadsheet as a way to track critical risks, generally include a column where a risk's "owner" can be named. The rationale for this practice is pretty clear: without assigning accountability, the likelihood of change in policy or practice is slim. Yet I find the concept a bit befuddling, especially since many risks are defined in unrealistically broad terms, such as "reputation risk." Using this example, it wouldn't be surprising to see reputation risk assigned to the Director of Communications at a nonprofit. Yet it's hard to imagine an organization where such a leader is able to capably and thoroughly monitor the landscape for reputation traps, forecast the ethical lapses of current or future leaders, or do anything to keep a good reputation safe. Many risks don't fit neatly into a single person's area of responsibility and require multiple 'owners' to act in a coordinated fashion to understand the issue and take action.

A Bird’s Eye View of Risk

Embracing Michael Power’s reference to ERM as “aspiration for a form of risk management practice which is all encompassing in scope, business-focused, and is suggestive of a bird’s eye view of organizational life,” offers a wonderful starting point for nonprofit leaders who recognize the potential value of a stronger and more inclusive risk management function in their organizations.

Many Center clients seem to relate to the benefit of a bird’s eye view of risk in their organizations. They admit that in some cases, the risk management function has become bogged down in departmental functions, with no connective strategy. For example, the IT team may be implementing safeguards to protect proprietary systems and confidential information and assume that as long as they are focused, their counterparts in other departments or offices have little need to understand the IT risk management strategy. A common precursor to a request for an ERM engagement is concern by a member of the executive team or board that risk may be falling between the cracks due to a siloed organizational structure and culture that inhibits communication, coordination, and collaboration across functional or departmental lines. This concern is particularly warranted for risks that straddle functions, departments or units and when teams feel pressure to keep their eyes trained to look for danger in the depths of their own silo.

Enlightened ERM

So what steps are recommended to embrace the benefits, while discarding the jargon of ERM? Here are a few thoughts to help you get started on a journey to strengthen risk management in your nonprofit. Whether you call it Enterprise Risk Management or RM 2.0, if you follow these steps you have a great chance to see an improvement in your program.

Step 1. Commit to the ERM Journey

Most organizations take 3-5 years to fully establish their ERM programs. While accountability structures and processes for identifying and managing risk can be quickly put in place, it takes much, much longer to make risk management part of your organizational culture where risk is consistently and systematically considered in every decision and action. Implementing ERM is very much a journey of culture change. That means you need to have some skills in leading culture change and plenty of patience. Don’t expect to get it all done in one easy step. Instead, start small and build incrementally. Take time to reflect and learn at each stage of development.

Step 2. Adopt a Shared Language

Begin your ERM journey by agreeing what the term means in your nonprofit. An all-encompassing approach to risk management that extends far beyond insurable risks? Risk management focused on risks related to strategy-setting? Risk practice focused on risk issues at the intersections of organizational life? It’s your choice. A word of caution: don’t adopt a definition that while authoritative and academic, has no real meaning in your nonprofit. Along with a definition of ERM, choose a definition of risk that works for your team.

Step 3. Be Ambitious, Opportunistic and Realistic

Don’t make the mistake of resolving to eliminate downside risks, or make every employee an enthusiastic risk champion. To ensure your efforts achieve buy-in, focus on risk management capabilities that help one or more key leaders resolve a pressing concern or difficult decision. Choose measurable but realistic goals for your ramped-up risk function. Add to that a timetable that won’t make everyone on the team feel like they are doing two jobs for a single paycheck.

Step 4. Celebrate Your Expertise, But Resolve to Learn

The ERM projects that are most likely to succeed are those led by people who are voracious learners—leaders who seek every opportunity to expand their knowledge and broaden their perspective on the discipline of risk management.

Step 5. Sidestep Groupthink with a Diverse Team

While the process takes longer when you bring together leaders with different world views and backgrounds, the ultimate result will be more meaningful and durable. Select members of the ERM team or task force for their differences, rather than similarities. Avoid the default approach to name every senior staff member to the ERM Committee.

Step 6. Start with the End in Mind

Although the long-term benefit of an ERM project is often hard to envision and even harder to calculate, it is possible to define how you will know that your labor has made a difference.

For example:

- When making decisions, leaders will consistently consider the associated risks, thereby giving context to the decision-making process
- Leaders will feel confident that key decisions are made with the best possible awareness and recognition of risk
- The board will feel confident in the thoughtful consideration of risks related to strategy in strategy setting and tactical plans
- Upgrading your current risk management program to one labeled eEnterprise Risk Management' is not simply about using a new acronym to dress up an old one. Embracing the idea of enterprise risk management and its associated concepts can be a wonderful first step to a stronger function, realization of important goals, and greater confidence about the risks you take to advance your mission. By recognizing and avoiding the missteps and embracing the six steps above, you will be in the best possible position to look back on your ERM upgrade as a worthwhile improvement.

Melanie Herman is Executive Director at the Nonprofit Risk Management Center. She welcomes your feedback and questions about the topic of Enterprise Risk Management at Melanie@nonprofitrisk.org or 703.777.3504.