

Property & Casualty Newsletter

September 2018: Enterprise Risk Management



What Is Enterprise Risk Management and Do I Need It?

Society grows more complicated every day, as does keeping your employees, equipment, and business safe. To cope with the proliferation of risks, we develop systems and technologies which, in turn, create their own risks. Successful long-term organizations learn to manage risk effectively and efficiently.

You have likely read or heard the term Enterprise Risk Management (ERM), but you may not be able to explain what it is or define it. ERM has become common at financial institutions, colleges, healthcare organizations, and federal agencies. Definitions of ERM differ by organization, but one of the most used comes from the Committee of Sponsoring Organizations (COSO):

“Enterprise Risk Management can be defined as the process affected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

My own personal definition of ERM is built around two main ideas:

1. Every Employee is a Risk Manager
2. The science and art of making risk informed decisions

The International Risk Management Standard ISO 31000 defines risk as “the effect of uncertainty of objectives.” This definition means that risks include both threats and opportunities. To ignore uncertainty would have the same result as driving through a large metropolitan area at rush hour with no traffic lights or stop signs: nothing happens and eventually tragedy occurs. No organization will exist long without some form of risk management.

You are already doing some risk management, and you may say “Okay, risk management is necessary, but do I need to develop an ERM program?” It is absolutely necessary to have enterprise-wide risk management to most effectively and efficiently reach your organization’s objectives, but a formal ERM program is optional. ERM is a tool that may or may not be helpful depending on how it is used. Use the term ERM if it is helpful, but if using it creates the perception of just another bureaucracy then do not use it.

Peter Bernstein’s 1996 book *Against the Gods: The Remarkable Story of Risk* makes the case that risk management has unleashed economic growth, improved the quality of life, and expedited technological progress. His premise is that using human reasoning, data, and probability mathematics when dealing with risk is both a science and an art.

The transformation is epitomized by the common reaction to Benjamin Franklin's discovery that lightning is electricity and can be controlled. Many of his contemporaries, who were educated and influential people, decried his claim, saying that lightning was a punishment from God and nobody could control or understand it. Yet within just a few years lightning rods were common in America and Europe with positive results: property preserved and lives saved.

I believe ISO 31000, the international risk management standard originally released in 2009 and updated in 2018, provides a fantastic model to help properly manage risk throughout most organizations. It is becoming the preferred model for organizations developing ERM programs. ISO 31000 has three primary parts:

1. Purpose and Principles (Mission and Core Values)
2. The Framework (Management Model)
3. Risk Management Process (Decision Model)

ISO 31000 is less than 30 pages long and is specifically written for use in all types of organizations. It contains some concepts important to successful risk management. Three of my favorites are:

- Significant risks need an assigned "risk owner": a specific person with ability and authority to control the risk
- Risk management should facilitate "risk informed decisions"
- All employees have risk management responsibilities



Wendell Bosen is a Senior Account Executive at Moreton & Company with over 25 years of risk management experience. He is one of six faculty for Public Risk Management Association (PRIMA) teaching workshops on ERM based on ISO 31000 across the country.

A good example of the ISO 31000 standard in action comes from my time as a risk management consultant for a commercial roofing contractor. I tried to convince the hot-tar foreman to clean-up the spilt tar each day, but he was measured by production time and had strong evidence that it was more efficient to clean up only after the job was done. What he didn't realize was the spilt tar slowed many other operations at the site, making other work less efficient.

Using a decision model similar to the ISO 31000 risk management process, the integrated risk was assessed and the best treatment was decided to be a daily clean-up of the tar. The tar foreman helped identify the risks and helped create the treatment so he was in full agreement with this treatment. As a bonus, he found a way to spill less tar!

If you would like to learn more about ERM or ISO 31000, contact your Moreton & Company agent today.

Please contact your Moreton & Company consultant with any questions.

Please visit www.moreton.com/news-events/ for more information and to view other newsletters. For additional questions, please contact your Moreton & Company representative.

© 2018 Moreton & Company. This newsletter is intended to inform recipients about industry developments and best practices. It does not constitute the rendering of legal advice or recommendations and is provided for your general information only. If you need legal advice upon which you can rely, you must seek an opinion from your attorney.

Moreton & Company - Idaho
2501 East State Avenue, Suite 200, Meridian, ID 83642
208-321-9300

Moreton & Company - Utah
101 South 200 East, Suite 300, Salt Lake City, UT 84111
801-531-1234
www.moreton.com

Moreton & Company - Colorado
4600 South Ulster Street, Suite 610, Denver, CO 80237
303-385-2100