ERM: Do You Know What it Means?

by
Richard W. Sarnie, CSP, P.E.

Risk and Insurance Management Society, Inc.®

Center of Excellence

Enterprise Risk Management (ERM) has received a great deal of media attention recently, but the concept is actually not a new one and has been silently prevalent for many years. It is only recently with the meltdown of the financial sector and the economic slowdown that it has begun receiving the tremendous amount of publicity. But with ERM being as important as it is to manage risk effectively, now is the time for anyone who must manage risk to learn about what ERM really is, how to implement it and what it can do for one's organization.

What is ERM?

My definition of ERM is holistic management of all material risk. Simply put, it is the view and identification of risk throughout the organization and the steps that are being taken to manage the risk. If you search for a definition of ERM on the internet, you would see many explanations. This can be very confusing because of the broadness of the definition; it means different action items and components for every single company.

What risk? How material to the organization? Define what is material to a company? What about corporate governance? Do I need a Chief Risk Officer? Is there insurance? Who should lead this? How do I begin? How much will this cost? What are the benefits?

There is No Magic Potion

The answer to the above questions is that it varies. There are many "experts" or persons that referred to them as experts in the field. This confuses and obscures the issue. There are books, articles, specialty companies and departments that are all dedicated to ERM. There is also an *ERM for Dummies* book dedicated to the topic.

This broad array of advice and differing opinions does not help companies, owners or organizations implement ERM. What needs to be understood is there is no magic potion or plan for Enterprise Risk Management to be implemented or effective within an organization. Companies need to define

their own process and customize it for themselves. Only then can a company begin the process of implementing a focused ERM plan within their culture.

The New Y2K?

Reflecting back to 1999, the world was concerned about what effect the date change was going to have with computer systems being programmed up until the date of 12/31/99 at 11:59pm. Risk managers and IT professionals can still remember reading about the prophecies of impending doom that were attached to the Y2K problem, and as a result, companies spent millions of dollars on consultants and studies of what impact could occur. There were many solutions created to protect against a potential Y2K catastrophe, and it gave rise to a cottage industry, the sole purpose of which was to help organizations deal with this potential worldwide crisis. Insurance companies went as far as to add Y2K exclusions to their insurance policies in anticipation of this event. Ultimately, the predicted crisis never materialized. But what it did do was force management to better understand their business and all the moving parts that affect it both internally and externally.

Why Now?

The buzz surrounding ERM has created a kind of new Y2K situation, with many organizations scrambling to understand ERM so they might create a program for it. This comes as no surprise, really—the world-wide recession in conjunction with the financial meltdown of several large institutions and government bailouts have brought the issue of Enterprise Risk Management to the forefront as a new concept. As a result, Standard & Poor's announced that it plans on evaluating a company's application and implementation of ERM as one of the credit rating factors when evaluating each individual organization. Standard & Poor's does not instruct companies how to implement and manage ERM; however they will evaluate how well the company defines risk and what systems are in place to highlight risks, get them to the proper level of management so they are addressed in a timely manner.

In actuality, the practice of ERM has been used by various successful companies for years as the way they run their business. Some risk practitioners have preferred to call it holistic risk management, rather than ERM. Some even may hold that any organization that manages itself properly does not need a Chief Risk Officer, or a Risk Czar. In this mindset, all risks boil down to money and most organizations either have a CFO (Chief Financial Officer) or a similar position responsible for managing, controlling and overseeing the company's monetary activities.

Such an outlook is likely to be debated by certain ERM practitioners, adding even more uncertainty to what is already a complex concept with multiple definitions. And as said before, this level of uncertainty can make it difficult, even intimidating, for even a seasoned risk professional looking to implement ERM at his or her organization. What is crucial to remember, however, is this: as important as ERM is, implementing it should not be as complicated or as daunting as it might seem.

Consider the example of a Fortune 500 company that had developed a mature ERM process that was complimentary to their practices and their culture. The company formed an Internal Committee called the Finance Council which was chaired by the CFO, made up of all the CFO's direct reports, their associates and the Business (Operations) Groups' Financial leaders. The CFO also invited the head of Investor Relations, the outside audit firm's senior partner and a representative from the General Counsel's office. This group met every six weeks and had a working session of discussing and publishing the risks of each division's business plan. The risks could be projected sales, new markets, supply chain, entry into new countries, etc. The CFO then would assign appropriate members of the council to work on these highlighted risks and report back at the following meeting on what steps were being taken to eliminate, mitigate or transfer those risks. This effectively covered all areas of risk the firm were encountering, and left little room for surprise or error. On an annual basis, the CFO reported the group's work to the Audit Committee and to the Board of Di-

rectors. Now consider that this example details a real-would example that practice took place over a decade ago and was simply standard operating procedure for the firm. The point is, ERM is no great mystery. It is simply a well thought out and implemented business plan with sound management processes in place.

Why the Confusion?

The reason for all the current discussion regarding Enterprise Risk Management returns to not having a set definition and the disarray that comes along with trying to decipher something you don't understand and utilize it simultaneously. I have seen companies trying to purchase computer software to identify and track risks. In addition, Accounting/Audit firms presenting themselves that they can help companies put into place ERM. My recommendation is that before spending money on software or accountants that referred to themselves as "risk professionals", there needs to be a fundamental understanding of ERM and the risks facing your Company first.

Keep it Simple

A good approach for implementing Enterprise Risk Management is to keep it simple.

- First, identify a champion (someone to lead and manage the process) in the organization. In many cases, the CFO (or better yet, the CRO) is the one who will lead this initiative. If the CFO or CRO is not qualified in leading this exercise, however, then engage the services of a competent risk management advisor who is well versed in ERM to help design and manage the process.

- The next step is to gather all the pertinent internal business leaders within the organization together and form a working group to manage the process and system.

- Define what dollar amount would be material to the entire organization. A loss of that dollar amount would either shut the company's doors or impact share price.

- Once the material dollar amount is identified, have each leader list what risks within their respective area could possibly bring about a material loss of that caliber.

- Have the group assign personnel to identify the steps needed to eliminate, mitigate or transfer that risk.

- Meet periodically to track progress against the action steps and continually define and improve the process.

- Once the material risks have been identified and steps put into place, the group then can broaden their definition of risk and begin the process of risk management for those non-material but large risks within their respective areas.

Conclusion

Once you have an Enterprise Risk Management process in place, it becomes routine for your company. ERM should not be a buzz word or a project (with a beginning and an end). It should be the way you manage your business today and tomorrow. More than anything, ERM is a way of life. ■

About the Author

Richard W. Sarnie, CSP, P.E. is the Senior Vice President and Chief Operating Officer of the ALS Group. The ALS Group is the premier provider of independent insurance and risk management services.

Rich has been with The ALS Group since 2008 and has over 20 years of risk management experience in the manufacturing, transportation and service industries. Rich was named the "Ideal Risk Manager" in 2005 by *National Underwriter* and was also profiled by *Risk and Insurance* as the "Zero Zealot" due to his unique and innovative approaches to risk management and loss prevention.

Rich has been a presenter and keynote speaker on numerous occasions at local and national risk management conferences and seminars. His topics have been on loss control, captives and creative risk financing techniques. Rich has a B.S. in Chemical Engineering from the University of Lowell (MA) and a MBA from Western New England College.

Rich is a Board Certified Safety Professional (CSP), a Construction Risk & Insurance Specialist (CRIS) and a licensed Professional Engineer (P.E.)

Rich is Licensed in New Jersey and New York as a Producer of Property & Casualty Insurance.

He is a professional member of the American Institute of Chemical Engineers (AIChE), the American Society of Safety Engineers (ASSE) and RIMS.

About RIMS

The Risk and Insurance Management Society, Inc. (RIMS) is a not-for-profit organization dedicated to the advancing the practice of risk management. Founded in 1950, RIMS represents more than 3,500 industrial, service, non-profit, charitable and governmental entities. The Society serves more than 10,000 risk management professionals around the world.

This white paper is published by RIMS with permission of the author and contributions from the RIMS ERM Committee.

For more articles, white papers and resources on enterprise risk management, visit the RIMS ERM Center of Excellence at www.RIMS.org.