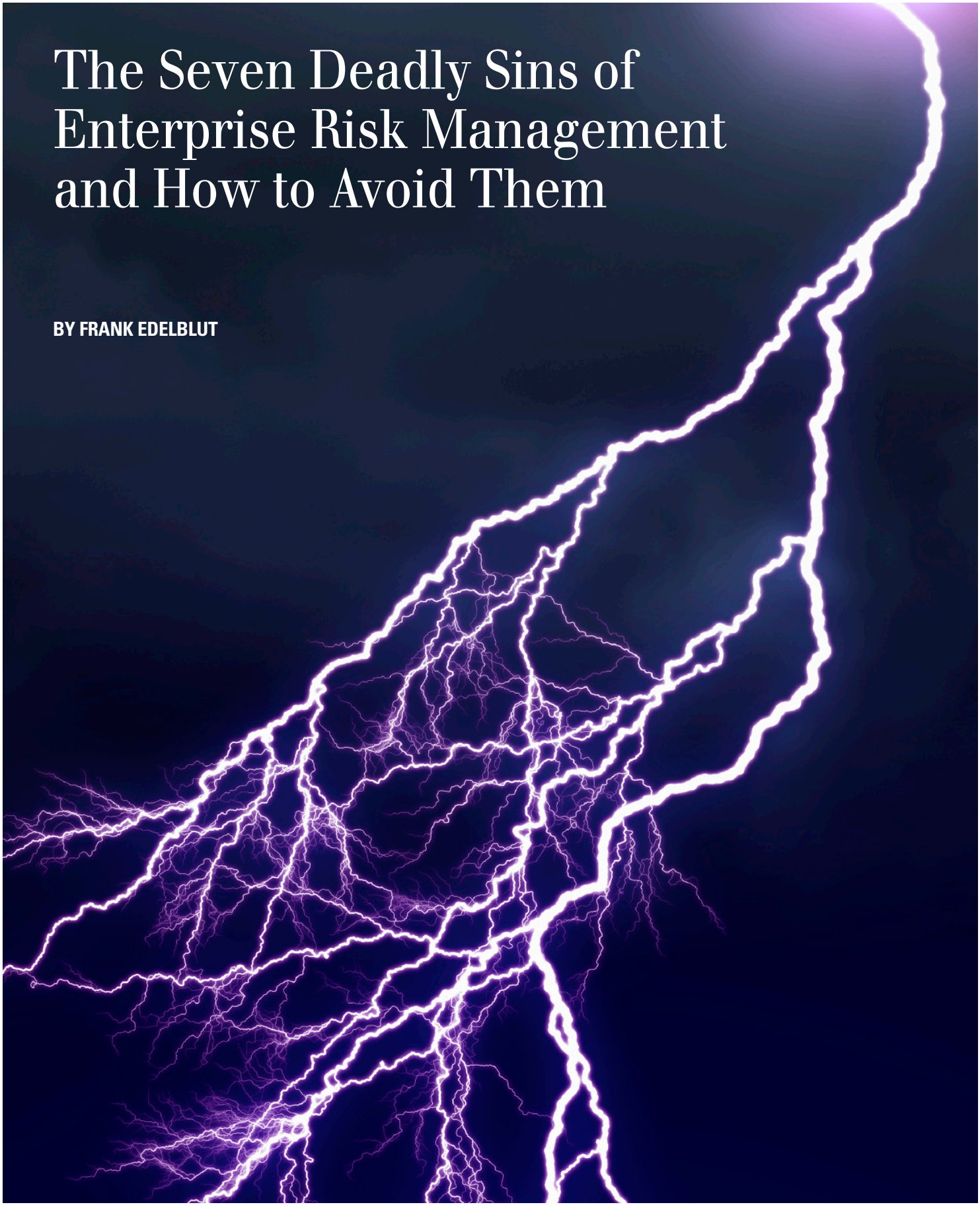
ControlSolutions®

The Seven Deadly Sins of Enterprise Risk Management and How to Avoid Them

BY FRANK EDELBLUT



Contents

Preface

Enterprise risk management — you've heard the phrase, possibly sat through a presentation or two on the subject. Perhaps you've even tried to implement it. Many organizations have been down this road already, some successfully and some not as successfully. However, you do not need to make the same mistakes as those who have gone before. In this paper we will highlight some of the more egregious errors others have made and the traps they have fallen into.

Background

Many point to the September 2004 work by the Committee of Sponsoring Organizations (COSO), Enterprise Risk Management – Integrated Framework, as the starting point for enterprise risk management (ERM). Certainly this was and remains an important work, one that has contributed significantly toward the advancement of the ERM agenda. Others mark the origin of enterprise risk management back in the 1970s along with the development of various management theories. Yet another perspective is that risk management is one of those "nothing new under the sun" topics; organizations were managing risk even before the early barter transactions when Rome traded olive oil and wine for lead, marble and leather from the Carthaginians.

Whether you view ERM as a recent development or not, it is clear that organizations have been managing risk (some better than others) forever! Anyone involved in line management has been making risk-based decisions on a daily basis. Recent developments in business have certainly brought the discussion of ERM to the forefront, but at its most basic level, risk management has always been part of the fabric of an organization.

We have all observed the pop-culture phenomenon that takes place when something or someone suddenly "makes it big." In the new place of prominence, some handle the pressure of the limelight well. Others buy expensive toys and trade "significant others" as though they were baseball cards. Like these people and ideas that suddenly make it "big time," ERM is at risk of becoming just another fad.

Consultants and academics alike have jumped into the ERM pool with both feet, increasing the possibility that ERM will lose its way. How does this happen? In an effort to "productize" ERM, consultants overengineer and complicate it to the point where it loses its true value proposition. Many leaders already recognize this and cringe at the thought of trying to tackle the subject. While business leaders perceive the inherent value of a structured approach to managing risk, they fear the "consultant-speak" that offers incredible promises but is likely to disappoint, based on experience.

However, it doesn't need to be this way. Many companies have successfully captured the benefits of ERM without empty activity that fails to deliver value. Whether you have already been disappointed or you are just now investigating ERM, you should look at the "seven deadly sins" of ERM. We'll attempt to help you sort through the mistakes others have made so that your ERM effort will remain on track.

111

Lack of a Clear Vision

One of the earliest mistakes that organizations make in their ERM initiatives is also one of the most common. And the frustrating aspect is that it is not unique to an ERM program but is a key component of any significant project: a clear vision for the effort.

This mistake manifests itself in subtle ways.

One Fortune 500 organization kicked off its ERM work because of increasing shareholder and stakeholder expectations. Another company, a large utility that had suffered a significant and highly public loss, needed to respond and demonstrate that they were doing something. The result was the initiation of an ERM effort.

Their activities were not designed to improve the business, but to respond to external pressure to act. Stakeholders are not the only source of pressure; it is clear that regulators are playing an increasing role in driving ERM. Companies listed on the New York Stock Exchange know well the current listing standards that require audit committees to "discuss policies with respect to risk assessment and risk management." These same requirements further state that "… it is the job of the CEO and senior management to assess and manage the company's exposure to risk …."[1]

[1] NYSE Listed Company Manual; Modified 11/03/04; Section 303A.00 Corporate Governance Standards; 303A.07 Audit Committee Additional Requirements.

External pressure will not subside anytime soon, as rating agencies and regulators alike are eyeing ERM to help them assess the organizations they oversee. Standard & Poor's (S&P) has already introduced ERM analysis into the corporate credit rating process, though as yet it is unclear how the information will be used.

While it is important to understand and meet external expectations and to address crises when they occur, these knee-jerk responses do not bode well for long-term, value-adding and sustained ERM. We have seen the effect on ERM initiatives that were started to meet external expectations. Even companies that begin these projects with enthusiasm (which is not always the case) often find that a competing expectation or another crisis develops. The result is that the ERM effort evolves into a rote exercise failing to deliver on the promises and expectations of the initial work.

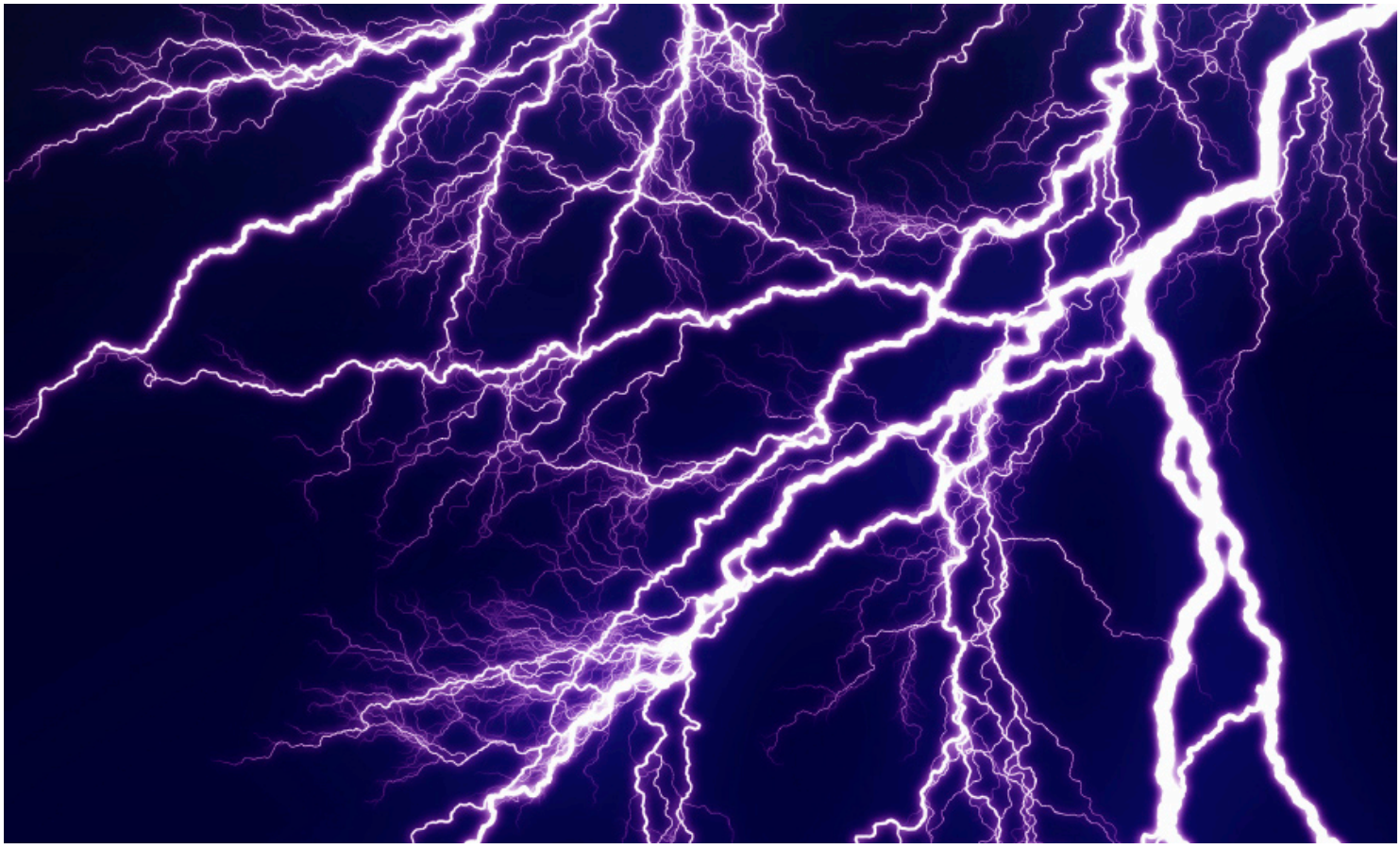
Management must have its own vision for ERM, one that is unique to the organization. The vision must be sustainable and focused on long-term value creation.

Building Unnecessary Organization, Function and Process

While lack of a vision for the ERM effort is the number-one reason why it fails to deliver on its promises, building unnecessary organization, function and process is a close second. As we discussed in the introduction to this paper, organizations have been managing risk all along.

While it is true that some have been doing this better than others, each one has been managing risk at some level. Everything you need for an effective ERM initiative already exists in your organization. There's no need to overcomplicate matters by rebuilding what you already have.

By not recognizing this, however, many companies launch into ERM by building new organization, function and process. At a large pharmaceutical company this resulted in the creation of a new risk management function. One Fortune 500 company described its reliance on a team of dedicated staff responsible for ERM and the development of new monthly, quarterly and annual reporting mechanisms. At this same organization, they described the continual challenge of making sure that the effort did not simply result in additional work for the field, a danger they readily recognized. Another organization described its goal of adding ERM to existing processes within the company.



In each of these examples, the underlying assumption was that risk management was a new activity to be added to the cost structure or something to be added to existing workloads. If one starts instead with the assumption that risk management already exists in the organization, then you will approach the project from a different perspective.

Rather than trying to determine what new function or process to create, you can start with identifying the risk management activities already in place within your organization. Once there is a good understanding of the current activities, then good decisions can be made as to the effectiveness of those activities and the need for any further infrastructure to connect them into an enterprise-wide and coordinated effort.

While in many cases it may be appropriate to create ERM functions and new process, if you start from that premise, you will undoubtedly add redundant function and process – and cost – to the organization. To avoid this you need to start with the assumption you already have many risk management activities embedded in your organization.

Lack of Support from Leaders

It almost seems silly to mention this because all of us recognize its importance in anything significant we undertake, but another common mistake is lack of leadership support for the effort.

Enterprise risk management activities are inherently influenced by the Risk Philosophy and Risk Appetite of an organization. Definitions for both of these terms come from the leadership of an organization. Some leaders have been deliberate in articulating the Risk Philosophy and Risk Appetite, while others hope that through osmosis the concepts will filter down and be understood by all. In any case, however, the leaders are influencing this whether they know it or not. If it is not self-evident, it is better to be deliberate about making certain that everyone is on the same page with respect to these key concepts.

Risk and risk management exist across the organization and at all levels. Risk does not discriminate between good performers and poor performers and is not influenced by management credentials or lack thereof. An effective ERM program eventually needs to be implemented across the entire organization. Without strong leadership support that aligns the organization around common Risk Philosophy and Risk Appetite definitions, there will not be a consistent perspective on or response to risk.

Bottom-up Approach

It must have something to do with the personalities of auditors and their love of detail. In spite of the obvious pain it was causing, most Sarbanes-Oxley compliance projects in the early years were worked from the most granular detail on up. Not surprisingly, many ERM efforts run by auditors have taken the same bottom-up approach, souring the experience for many who are still sensitive and wary of company-wide initiatives coming from the finance organization.

One B2B products company described its early approach in this way. The first step was to create a Risk Model and deploy an online risk identification survey to identify the top risks. This produced a large list of potential risks that might face the organization, which was followed by a two-day workshop with executive management to further understand and evaluate the core business risks. In addition, face-to-face interviews were conducted with executive management.

Another organization described its efforts as a bottom-up survey of risks, which were then entered into logs used for tracking. The auditors regularly went back to the organization to refresh the risk universe. The result was a list of over 2,000 monitored risks.

Driving this approach is the classic risk question asked by auditors around the world: "What could go wrong?" or, alternatively, "What keeps you up at night?"

The important mistake to avoid here can be illustrated, again, by a familiar Sarbanes-Oxley experience. Through a bottom-up approach to identification of Internal Control over Financial Reporting (ICFR), the population of key controls grew disproportionately to the objectives of ICFR. Simply stated, most organizations identified too many controls; in later years, applying a top-down approach, they were able to reduce the number. Had a top-down approach been applied from the beginning, only the most important controls directly connected to the objectives of ICFR would have been included.

Now apply the principle to ERM. By taking a bottom-up approach, organizations are including many risks that may or may not actually manifest themselves in the business. Companies are incurring inordinate costs to identify, log, assess and monitor risks that are unlikely to occur or cannot be mitigated.

The fundamental flaw here is a failure to apply the COSO approach. The objective of ERM is to help organizations meet their stated objectives. This is accomplished by managing the risk that might prevent the achievement of the objectives. Thus, a top-down COSO approach starts with the objectives, not with the risks. We have discovered a simple but effective way to accomplish this, and it lies in the question asked. Rather than asking "What might go wrong?", consider asking "What must go right in order for the company to achieve its objectives?"

In a conversation with an executive of a large waste management company, he identified the greatest risk to his future as the failure to execute against his strategy. By asking the question "What must go right?" we are more clearly able to identify those activities that must affirmatively happen in order to meet the strategic objectives of the company. Asking the question "What might go wrong?" may lead you to the correct risk, but it will almost certainly also add risks that are not directly connected to achievement of strategic objectives.

Risk Confusion

When first entering the arena of ERM, you are bombarded by new nomenclature, the most prevalent of which is the word risk followed by something: Risk Philosophy, Risk Appetite, Risk Tolerance, Risk Assessment and Risk Response, to name but a few. (I also recently heard a new term, Risk Environment.)

The mistakes that organizations make with respect to these terms are twofold.

The first is failing to recognize that these are not interchangeable terms that can take on any definition we want them to have. Each has specific meaning in the context of COSO ERM. Each plays an important role in ERM, yet many people substitute one for the other, either out of ignorance or lack of care. That brings me to the second mistake. Each of these terms needs to be defined and agreement reached within the organization as to how they will be used. We've all been in meetings where the person using a term means one thing and the hearers understand something different. Without a common language, miscommunication will be inevitable, resulting in wasted time, effort and resources for your company.

Consultants and other outside organizations are complicit in adding to this lexicon confusion. For example, one of the questions posed by S&P with respect to ERM is: "Is there a statement of risk appetite or risk tolerance?"[2] Without a strong understanding of COSO ERM, one might not recognize how this question goes astray.

[2] Standard & Poor's; "S&P Extends Comment Period On Enterprise Risk Management-nalysis For Nonfinancial Co. Ratings"; January 14, 2008; page 2.

While both Risk Appetite and Risk Tolerance deal with the amount of risk an entity is willing to accept, they are different concepts which in practice do not comingle as easily as S&P has implied here. Risk Appetite is a component of a company's internal environment and a "higher level statement that considers broadly the levels of risks that management deems acceptable."[3] Risk Tolerance, however, is a component of objective setting in the COSO model, reflecting the measure put in place to determine achievement of specific strategic objectives. "Risk tolerances are more narrow and set the acceptable level of variation around [specific] objectives."[4] While it could be possible to distill a single Risk Appetite statement, Risk Tolerance can only be expressed in the context of a specific strategic objective. A company may have one Risk Appetite statement but would have many Risk Tolerance statements in support of its multiple objectives. So, you can see it makes no sense to ask "Is there a statement of … risk tolerance?"

[3] COSO; FAQs for COSO's Enterprise Risk Management — Integrated Framework, point C1; http://www.coso.org/erm-faqs.htm.

[4] Ibid.

Overly Complex Risk Assessment

Once the important risk events have been identified, some type of prioritization is required to allow the organization to allocate finite resources to the most important areas. We see two common mistakes in the Risk Assessment process that are closely related.

The first deals with complexity in the quantitative analysis of risk events. And, it is not so much the complexity, but rather the perception that by using a complex approach to assessing risk, the outcome will somehow be better. The reality, however, is that management qualitatively has a good sense for risk – remember that they have been managing it all along. The result we have seen is management simply manipulating the quantitative models to render the outcome they expect. While this manipulation does generally result in the correct risk assessment, why create the perception of quantitative analysis if the end result is qualitative?

The second mistake is making Risk Assessment the most important part of the process. One energy company described Risk Assessment as the "foundation" for its whole ERM process, and another described it as the "building blocks." The result of this imbalanced approach is a disproportionate allocation of resources and time to the assessment effort and the potential for quarreling among management on the correct prioritization. While time spent on important aspects of ERM are cut short, significant time is spent determining the likelihood and significance of each risk event.

The discussion ensues something like this: "I think it is a 3"; "No, I think it is closer to 3.5" (on a scale of 1–5, of course). Interestingly, many of these discussions about likelihood and significance fail to incorporate a holistic view of the company. Little recognition is given to an organization's relevant experience and capability to respond to a specific risk event. An event may be both likely and significant, but if an organization has dealt successfully with the same or a similar issue many times in the past, the residual risk – risk left over after considering this history – could be low, changing the response that management might make.

Any prioritization of risk must recognize the importance of management's qualitative input. When using a "What must go right?" approach (discussed under the point on Bottom-up Approach above) and considering the organization's capacity to respond to the event along with likelihood and significance, it is easier to come more quickly to effective assessment of the risk and allocation of valuable resources.

Making ERM the Endgame

COSO guidance puts it this way: "Enterprise risk management helps an entity get to where it wants to go and avoid pitfalls and surprises along the way."[5] The common and understandable mistake made by many organizations today is to allow ERM to take a higher priority than it should. ERM should support an organization's ability to "get where it wants to go" or meet its strategic objectives. Often, however, ERM is playing too important a role, either alongside strategy and objective setting or, in some extreme cases, trumping strategy and objective setting.

In a recent association meeting of company directors, including audit committee members, there was near-unanimous agreement that they are contributing more and more hours to the companies they serve. However, less time is spent now on strategy and objective setting and more time is spent on issues of compliance and risk. If, in times past, the ratio of working on company objectives versus compliance issues was 80%/20%, today it is the reverse. ERM is contributing to that. Properly deployed, ERM should support and help ensure achievement of strategic objectives. It cannot become an objective unto itself, which is the trap that many companies fall into. One products company described it this way: "Whereas some organizations establish ERM as a separate function, with its own set of priorities and action plans, we decided to link the ERM process to our strategic planning processes."

[5] COSO; Enterprise Risk Management – Integrated Framework, Executive Summary; September 2004; page 1.

Conclusion

ERM has the capacity to deliver exceptional value back to an organization that effectively deploys the COSO methodology. Yet even the COSO methodology can seem or become complex and convoluted in its application. The result is that you may make the mistakes we have described here – the "seven deadly sins."

To be effective, ERM must start with a big-picture perspective, through which we define the environment into which any ERM effort will fall. COSO refers to this as the Internal Environment, and it includes the concepts of Risk Philosophy, Risk Appetite and the all-important Entity Level Controls we spent so much time on during our Sarbanes-Oxley compliance work. Within this Internal Environment we can build an effective ERM program.

ERM must start with the organizational objectives – what, as an organization, we are trying to achieve. Knowing that gives us the goal. We then need to define our Risk Tolerance, which, as described above, is nothing more than the performance measures that tell us whether we have met our stated organizational objectives. Moving on from Risk Tolerance, we must identify the events that are most important to achievement of our objectives within the Risk Tolerance – the "What must go right?" question. This is followed up with the oversight aspects of ERM and links the system of internal control of an organization to the achievement of its organizational objectives. Oversight includes the control activities we put in place to make sure that what must go right actually does. These controls feed information into the organization about events, and the information is monitored to ensure an effective response to nonconforming events.

Reactions from the marketplace are mixed as to the efficacy of ERM. All agree on the value of managing risk, but many have become disillusioned through consultant-speak on the topic that promises value but fails to deliver. Much of that failure stems from these "seven deadly sins" of ERM – mistakes made by real companies that have caused their ERM programs to come up short. You can learn from them and understand them so that you don't have to make the same mistakes. The key is to keep your ERM efforts simple and focused.

ABOUT THE AUTHOR

Frank Edelblut is chief executive officer of Control Solutions International, a leading global provider of independent internal audit, compliance, risk management and technology solutions.

He is the creator of the OREO™ COSO-based ERM methodology, which has been titled by some as "ERM Made Simple." Using a simple and practical approach, he has captured the essence of COSO ERM in a way that no one else has. One consumer products company that had been working with a Big Four methodology for two years stated, after understanding OREO, "This is what we have been looking for and what has been eluding us for the past two years. We have built so much process and infrastructure using the [Big Four] model, but we are no closer to managing our risk than we were before we started."

ControlSolutions®

The leading global risk and control solutions advisory firm.

www.controlsolutions.com

AP6610L