Orion constellation
volume 7 number 1
winter 2009

The Seven Deadly Sins of Enterprise Risk Management

...and how to avoid them

Recent developments in business (financial crisis, etc.) have certainly brought the discussion of Enterprise Risk Management (ERM) to the forefront.

Whether you view ERM as a recent development or not, it is clear that organizations have been managing risk forever! Anyone involved in line management has been making risk-based decisions on a daily basis.

With all of the hype and mixed messages in the marketplace, enterprise risk management is at risk of becoming just another fad. 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.

1. Lack of a Clear Vision

In most cases, this mistake occurs because ERM is initiated in response to external pressure, 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.

While it is important to understand and meet external expectations, management must have its own vision for ERM, one that is unique to your organization. The vision must be sustainable and *focused on long-term value creation*.

2. Building Unnecessary –and Costly– Organization, Function and Process

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.

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.

3. Lack of Support from Leaders

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. 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.

(continued on page 2)

Navigating Your Organization's Future

ORION DEVELOPMENT GROUP
177 Beach 116th Street, Suite 4 • Rockaway Park, NY 11694
Phone (800) 510-2117 • Fax (718) 474-8210 • E-mail: info@odgroup.com • Web: www.odgroup.com

The Seven Deadly Sins of ERM *(Continued from page 1)*

4. 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. 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?"

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. 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?"

5. 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.

> Whereas some organizations establish ERM as a separate function…we decided to link the ERM process to our strategic planning processes."

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 needs to be defined and agreement must be reached within the organization as to how they will be used. For instance, while both risk appetite and risk tolerance deal with the amount of risk an entity is willing to accept, they are different concepts in practice. 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." 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. While it could be possible to distill a single risk appetite statement, a company will have many risk tolerance statements in support of its multiple objectives. So, you can see how this can cause confusion and rework.

6. 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 is 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 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. The result of this imbalanced approach is time spent on important aspects of ERM are cut short while too much time is spent determining the "precise" likelihood and significance of each risk event.

7. 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." The common and understandable mistake made by many organizations today is to allow ERM to take a higher priority than it should. If, in times past, the ratio of working on company objectives versus compliance issues was 80%/20%, today it is the reverse. ERM should not become an objective unto itself. 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."

(Continued on the next page)

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.

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. ■

New ERM Seminar

The University of Virginia is offering an *Enterprise Risk Management* seminar on March 31-April 1, 2009 in Falls Church, Virginia. The cost is $1,195 per person.

This practical two-day seminar delivers a top-down, step-by-step process to:

- Balance opportunity and risk when setting strategic objectives
- Determine the appropriate risk tolerances for specific objectives
- Identify events that can undermine strategic objectives or the organization as a whole
- Integrate the oversight of strategy deployment and risk via the balanced scorecard

For more information or to register, go to http://odgroup.com/seminars/enterprise-risk-management/index.asp.

Moving Into The Hall of Fame

Weichert Relocation Resources Inc. (WRRI), one of the world’s leading relocation and assignment management companies and a client of Orion Development Group, has been inducted into the 2008 Palladium Balanced Scorecard Hall of Fame™.

WRRI is the first relocation and assignment management company to receive this distinction. (Another Orion client, Alcoa CSI, was a Hall of Fame finalist two years ago.) “It’s a distinct honor to be recognized by the Balanced Scorecard Collaborative for our success in executing strategy,” said Aram Minnetian, president of WRRI and architect of the company’s BSC Enterprise Model.

Congratulations Weichert! A profile of WRRI will appear in the next edition of *Constellation*.

Doing More With Less – NEW SERVICE

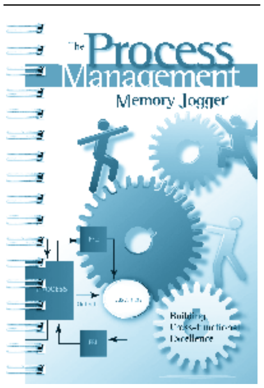
In these lean times, organizations in every industry and sector are being asked to tighten belts. One unfortunate side effect of budget cuts is the reduction of value for your customers. This creates a downward spiral that is hard to escape.

Fortunately, Orion knows the answer! Our process optimization coaching will help you eliminate waste without cutting customer value.

Please go to www.odgroup.com/optimize.asp to view our targeted consulting solutions that will help your department, agency or company do more with less via process optimization.

New for 2009
Get a 25% Discount Until February 13th

The latest installment in the famous Memory Jogger™ series, *The Process Management Memory Jogger*, is now available. This "how to" book explains tools and techniques that will enable you to:



- Clarify and focus on what is of value to the customer
- Improve cross-functional coordination
- Maximize the competitive impact of process performance
- Map and streamline workflows
- Explore the logic how work is done
- Create better process improvement solutions
- Align processes with IT systems

For a limited time, the publisher is offering a 25% discount off the $17.95 list price of this brand new pocket guide.

Visit http://www.goalqpc.com/shop_products_detail.cfm?PID=1059 to order. Mention **Promotion Code 019G1** to get your 25% savings!

Memory Jogger is a registered trademark of GOAL/QPC.

ORION DEVELOPMENT GROUP
177 Beach 116th Street, Suite 4
Rockaway Park, NY 11694

Presort Standard
U.S. POSTAGE
PAID
East Lansing, MI
Permit #21

Inside. . .

- **Seven Deadly Sins of Enterprise Risk Management**
- **New ERM Seminar**
- **Moving into the Hall of Fame**
- **Doing More with Less - *A New Service***

This is your newsletter. . .