

# Effective Enterprise Risk Management

Douglas A. Nagan  
Albert C. Patterson, IV

We hear about major risk management failure on a regular basis. Recent examples include: Boeing's 787 Dreamliner wing components, Toyota's acceleration system, Boston Scientific's patent infringement, and BP's oil spill. These failures cost billions of dollars, plus negative impacts to reputations, growth and stakeholder value. Directors need to understand major risks, so they can independently validate senior executive claims. Senior executives need to understand major risks so they can better manage them. It's time for visionary corporate leaders to implement enterprise risk management programs that work.

Over the last 2 years, we analyzed many of the high-profile risk management failures and determined that most failures can be traced to the following:

- **Static** enterprise risk management programs.
- **Generic** programs that provide inadequate risk management information and partially integrated risk management frameworks to senior management.
- **Amorphous** ERM ownership leading to operational risk gaps and silos and cultural risk awareness deficits.

An ERM Program should provide directors and senior executives with a process to significantly improve risk management, business resiliency, financial performance, growth and stakeholder value. A fully functioning, well-integrated enterprise risk management program also improves competitive advantage.

The old adage is true - the fastest cars need and have the best brakes.

Enterprise Risk Management (ERM) programs generally follow a structured process that includes determining risk identification, risk sizing, risk appetite, risk remediation, and the creation of recovery and continuity plans. This process, following generally accepted guidelines, is expected to cover all the bases. However, organizations are all too often faced with unexpected risks without adequate responses at hand. Such unexpected risks may not have been possible to foresee or they could result from incomplete analysis that if more comprehensive would have identified them. While there can be many reasons for ERM programs to fail there are some common threads. Specifically ERM programs that fail tend to have one or more of the following in common – the plans were static, the plans were generic, and finally ownership of ERM was amorphous and likely the enterprise's culture did not include risk management as a practice.

## What do we mean by this?

**Static** means the ERM programs and plans that were created are viewed as objectives that once reached means the task is complete. The reality is that from the very moment such plans are published they begin to lose effectiveness as change occurs and new risks arise. Is this change fast and comprehensive? No, but it is inevitable. As an example British Petroleum's latest 20F SEC filing [the equivalent of a 10K filing for non domestic companies] has the following statement under Operational Risks/Drilling and Production, ' . . . We may be required to curtail, delay or cancel drilling operations because of a variety of factors, including unexpected drilling conditions, pressure or irregularities in geological formation, equipment failures or accidents, adverse weather conditions and compliance with governmental requirements.' It is easy to imagine the wording of the next 20F filing will include a statement relating to environmental damage and damage control procedures.

**Generic** describes plans that are developed from templates or industry standards such as COSO. The problem arises when templates and standards that were developed to reflect generalized normative situations are applied without appreciation of the unique characteristics and requirements of a particular organization. For example have you heard the statement – 'We are COSO compliant' as though that is a sufficient criterion. As an

# Effective Enterprise Risk Management

Douglas A. Nagan  
Albert C. Patterson, IV

example, Boeing in its 10K filings says it has built its entire internal policies and control procedures around the COSO standard yet they have had numerous failures in creating product and ethical conflicts in gaining contracts. Standards are a good beginning point but for an ERM plan to be effective it must reflect an organization, its markets, values, culture, operations, business partners and environment.

**Amorphous** ownership means the ERM program is diffused across the organization with few clear lines of responsibility and the ERM programs are not integrated into the organization's standard management reporting systems and objectives. This means the ERM will be viewed by line managers not as one of their prime responsibilities and therefore ERM will receive minimal attention. For example Boston Scientific's latest 10K dated March 26, 2010: 'We believe that our risk management practices, including limited insurance coverage, are reasonably adequate to protect against anticipated product liability and securities litigation losses.' Yet 10 days earlier they had to do a full product recall of their key product, defibrillators, and saw their market value plunge by 12.5%. One has to wonder who was responsible for the 10K and who was responsible for the recall. Clearly they were not communicating.

## How can we address these issues?

For an Enterprise Risk Management program to avoid these pitfalls it needs to be:

- Adaptive – The ERM program needs to evolve with the changes that occur in the organization, risks, markets, technology, regulatory environment and society.
- Culture<sup>1</sup> – The ERM program needs to reflect, understand, leverage, work within and modify as necessary, the culture of the organization. The mindset must be "we will actively and constantly identify and manage the risks in our enterprise".
- Metrics – The ERM program needs measures that reflect the various risks and are part of the organization's standard goals, objectives, and reporting process

Adaptive - In order to address the issues raised in a static ERM you need to adopt an approach that evolves with the changes that occur. We call this an adaptive approach.

*'It is not the strongest of the species that survives, nor the most intelligent, but the one that is most responsive to change'*  
Charles Darwin

This means an effective ERM needs to include:

- Periodic scans of internal operations and procedures, suppliers, competitors and customers to determine if any changes have occurred that will require changes to your ERM. Scans of suppliers and competitors are sometimes done as part of an organization's sales and marketing efforts and might be able to be used without major effort to include items relevant to ERM. As changes are identified they then need to be integrated into the ERM plan.
- Formal review mechanisms to make sure the ERM is updated on a regular basis. These reviews to have credibility need to be done at the board level.
- Drills to make sure the procedures and processes to contain risks actually work. While many parts can be tested on a standalone basis it is important to have an occasional broader test to verify the cross organization support is working properly.

---

<sup>1</sup> Culture is the collection of beliefs, values and behaviors that are common to an organization

# Effective Enterprise Risk Management

Douglas A. Nagan  
Albert C. Patterson, IV

Culture – For an ERM effort to be effective it must be part of the culture of the organization. This means it must become part of the specific values, beliefs and objectives of the organization and communicated throughout the organization.

*“When I started at IBM I thought culture was important; when I finished I realized that it was the only thing that was important.”  
Lew Gerstner from Who Says Elephants Can't Dance.*

In order to do this you need to understand that culture matters, culture can be measured, and that culture can be managed.

- Culture matters is best explained by considering several examples. A widely agreed upon reason for Toyota's product recalls with all the attendant fall out is that Toyota changed its culture from one with a quality focus to one of financial cost control. There are numerous examples of corporate cultures that become fixated upon a single vision and do not change as circumstances changed. Think of Polaroid and DEC.
- Culture can be measured by realizing that culture is composed of a number of attributes (such as is the organization's perspective strategic or tactical, does it view itself as evolving or more static, how are individuals recognized, and is the focus more on achievement or adhering to a process). Each attribute has range of measurable qualities that allow absolute and comparative metrics which can be used to create a culture profile.
- Culture can then be managed because what you measure you can manage and what you manage you can change. The measures can be used to compare profiles across the company, watch profiles change over time, determine desired profile and develop plans to achieve such.

The relevance of being able to measure and manage culture can be summarized as follows:

- An organization's culture is critical in maximizing the effectiveness of its ERM program.
- Conflicting cultures within an organization can stifle the best of ERM plans
- A dysfunctional culture, one that is not aligned with corporate goals and objectives, will keep an organization from realizing its potential, including ERM

Metrics – The implementation and use of measures that describe an organization's ERM preparedness is critical to the success of any ERM program.

*“I often say that when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science, whatever the matter may be.”*

*Lord Kelvin from his 'Lecture on "Electrical Units of Measurement" (3 May 1883)*

There are several key points regarding ERM metrics.

- ERM metrics need to be integrated into the organizations objectives and reporting process.
- ERM metrics need to apply at all levels with metrics that relate to the specific job and responsibilities.
- ERM metrics need to include the risks the organization faces including likelihood and severity, preparations and plans in place, completion of plans, reviews and tests.