Getting the Focus on Enterprise Risk Management Right

by
Al Decker &
Donna Galer

Risk and Insurance Management Society, Inc.®

ERM
Center of Excellence

Definition and Purpose of Enterprise Risk Management (ERM)

All business processes exist to achieve a specific end product or objective. ERM is a business process; not an end unto itself. Its objective is to better ensure the sustainability of an organization and enable it to meet the goals set forth in the organization's strategic or annual plan.

A typical approach to ERM begins with a focus on current or future organizational risks. This often begins with a focus on the business plan and what may prevent it from being achieved. Although risks often have a strong downside potential, they can also present opportunities or upside potential. Both types should be identified. Then, through assessment and prioritization, small/unlikely risks are separated from large/likely ones.

In the practice of ERM, risks are identified, and responses to them are developed, holistically across the organization and responses to them are developed. The response may be in the form of risk transfer, amelioration, elimination or positive exploitation, so that the organization can place itself in a better position to meet its planned profitability goals. Thus, the risks may be insurable or not, may be current or emerging, may affect the entire business or only a portion.

Benefits of an Enterprise Approach to Risk Management

Among the benefits of practicing ERM include:

- Helps ensure that business goals and objectives are reached
- Improves management's ability to understand and manage risk
- Assists in reducing the impact of risk and of adverse events that do occur
- Positively impacts rating agency assessments
- Enhances the organization's ability to deal with legal actions related to their response to risk
- Aids in maintaining an organization's competitive advantage and good reputational image

ERM is a Process

As a business process, ERM requires a framework and step by step methodology for implementation. This article will address both. As the ERM process moves from one step to the next, there are inflection points that require management's strategic thinking, operational knowledge and decision-making. Various output will be produced that become business tools for tracking risks and the action plans for addressing these risks.

One way to think of the overall process is to consider the categories rating agencies use when assessing an organization's risk management approach. When evaluating insurance companies, for example, S&P has been using the following categories according to David Ingram[1]:

1. Risk Management Culture
2. Risk Controls
3. Emerging Risk Management
4. Risk and Economic Capital Models
5. Strategic Risk Management

Organizational Culture Must Support ERM

As published in the John Liner Review, "In answer to the question 'What is the most important aspect of ERM as distinct from former models of RM?', Roy Fox, director of enterprise risk management at Bonneville Power Authority in Portland, Oregon, said, '"It is a cultural distinction; there needed to be a mind expanding approach to viewing risk'".[2]

What creates a particular culture, or a subset of culture, are:

- Messages sent from the top of the organization
- Processes that are implemented
- Investments in tools and reporting to support the process
- Recognition and Rewards, especially compensation criteria

[1] ERM-II RESEARCH REPORT: Enterprise Risk Management for Property-Casualty Insurance Companies," Shaun Wang and Robert Faber.

Any pervasive process in an organization requires a cultural underpinning for the process to rest upon. When a group shares a common set of norms or beliefs, a culture is born. To foster a culture that values ERM, there would have to be a shared belief that risk is an important business factor. Further, the belief system would have to recognize it is “ok” to raise risk related issues, fostering a cultural understanding of ERM as an integral part of meeting business plan goals, as a process not a control. There would also be democratization of responsibility for identifying and handling risk across all staff in an organization.

Added to all this, a common vocabulary is needed so that communication is clear and relevant. At the end of the day, for ERM implementation to be successful, the entire organization has to get some level of education about risk and the steps in the ERM process.

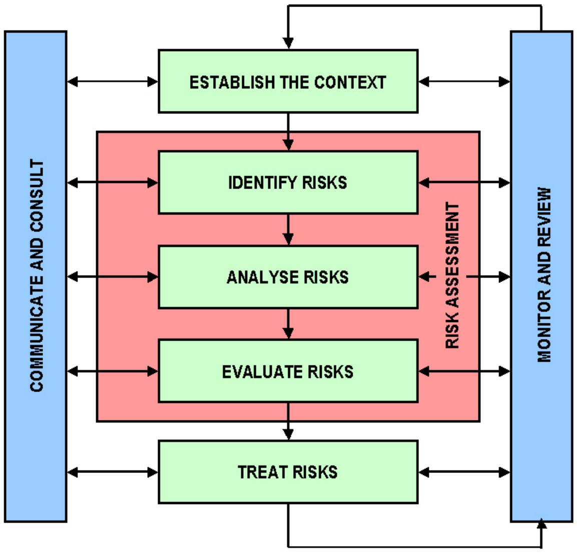
This education may need to begin with the Board or senior management and then cascade through all levels. The form of education may be different, depending on the organization. However, all forms should include some sort of documentation that the learning has been affected; this could be a sign-off or a completed e-test.

And, the ERM Process Must Have a Foundational Underpinning

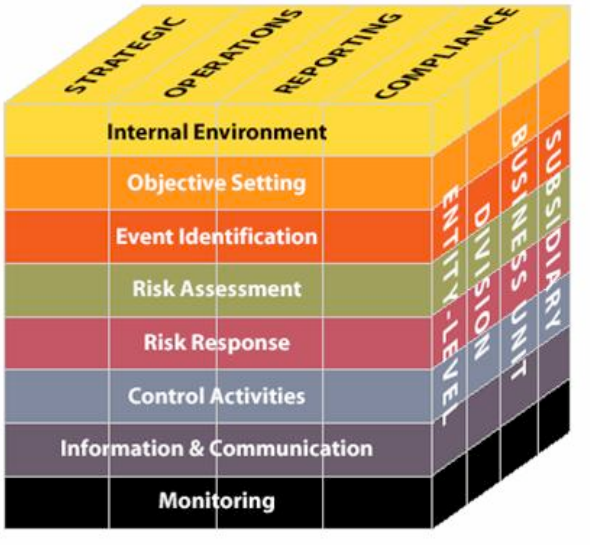
There are two internationally accepted frameworks or standards for ERM, ASNZ 4360-2004 and COSO ERM. Another framework, ISO 31000, is currently under development. The framework forms the foundation for the ERM process.

Here is a pictorial view of these standards:

[2] Donna Galer, “Clearly Differentiating Between Old and New Models of Risk Management: A Discussion of ERM Today,” *The John Liner Review,* Vol1, No 4, Winter 2008.



ASNZ 4360-2004



COSO ERM

The ASNZ describes ERM as:

> Risk management involves establishing an appropriate infrastructure and culture and applying a logical and systematic method of establishing the context, identifying, analyzing, evaluating, treating, monitoring and communicating risks associated with any activity, function or process in a way that will enable organizations to minimize losses and maximize gains.[3]

COSO ERM describes ERM as:

> Enterprise risk management is a process, effected 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.[4]

[3] "Standards New Zealand Technical Committee OB-007 "Australian and New. Zealand Standard on risk management, AS/NZS 4360" (:2004).

[4] Committee of Sponsoring Organizations of the Treadway Commission, "Enterprise Risk Management — Integrated Framework" (2004).

Selecting a Framework

Selecting one framework and applying it across the organization establishes a common language and understanding of risk, significantly enhancing the organization as ability to effectively communicate risk, opportunity, mitigation and prospects. It ensures:

- a common ground and discipline
- consistent approach and point of view
- allows the approach to be applied at a macro as well as a micro level
- a foundation of a common dialog across levels of management
- a holistic view of risk

In addition, adopting an internationally recognized framework not only creates a basis for internal and external credibility, but potential ease of alignment with laws or industry requirements that are likely to evolve.

Because ASNZ is so clear and because it better stresses the need to take a not only an internal but also an external view of risk, it is one that the Business First TM prefers.

Organizational Structure

The ERM mandate should come from the Board or CEO. There needs to be a process owner and that normally is the Chief Risk Officer or Risk Manager. If neither of these roles exists in the organization, the process owner might be someone from Operations or Finance. The process owner will form a Risk Committee made of knowledge experts from various staff and operational functions in the organization to help with core steps in the process such as risk identification, assessment and mitigation.

In essence, there is little need to create another organizational unit or hire a lot of new staff. The one new element is the Risk Committee, made up of current functional and operational managers.

Business First, Risk Second

Too often, ERM programs are initiated to satisfy some compliance requirement, or at the insistence of a board member of officer, or simply because it seems like the right thing to do. When the ERM program is viewed as the end product, however, the company can lose its advantage as a significant strategy tool to help ensure results and expected outcomes are achieved. Only when the ERM program is strategically linked to the overall business plan and execution, does it gain true value and become a meaningful exercise and a means to an end. To achieve this, an organization needs to take a structured approach to designing and implementing their ERM process.

The first step involves a review of organizations business plans not the development of a long laundry list of risks that might affect the organization. Thus, business comes first, not risk.

What follows a circular chain of considerations that ultimately feeds back upon itself, with no true beginning or end. It is a closed cycle, perpetually renewing itself:

- CEO establishes mandate

▼

- Risk committee is formed

▼

- ERM education starts

▼

- Process is launched

▼

- Improved monitoring and reporting of risk

▼

- Embedded in performance management,

▼

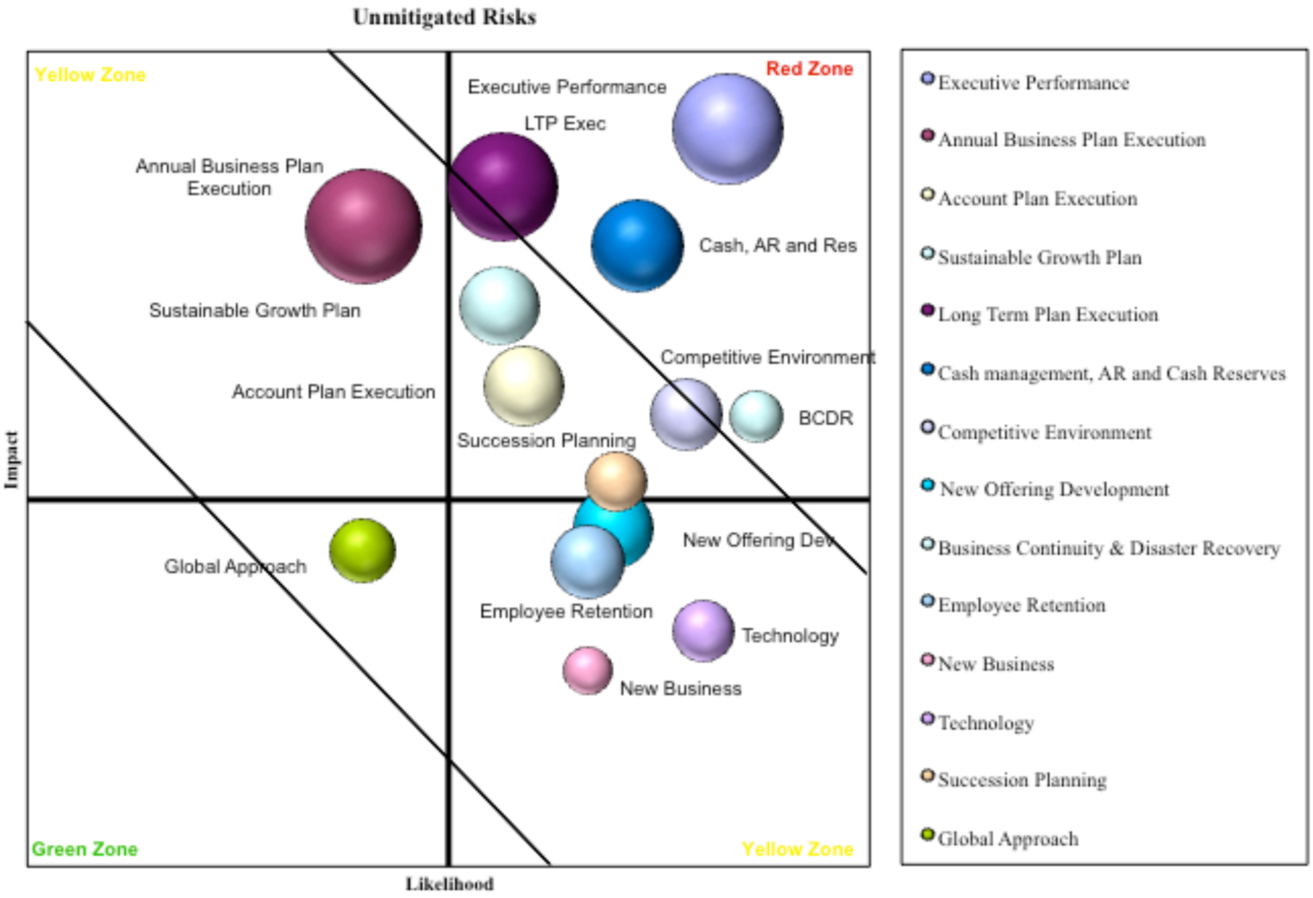
- CEO establishes mandate...

Process Steps

1. Select most important elements of organizational strategy and goals. As described in ASNZ-4360 the organization needs to establish the context for the ERM Program. In Business First TM ERM the context are the business initiatives and goals that must be achieved in order for the overall strategy to be successfully accomplished. All business plans include certain initiatives that a company must do well in order for the strategy to be achieved. Initiatives such as modernizing technology, maintaining high quality executives and human resources while minimizing turnover, increasing sales and market share are all necessary to achieve success. In this step, some of the questions to ask are: 1) why are these initiatives important to the success of the plan, 2) which of these initiatives are most important to the organizations success, 3) what information do we have about these? The initiatives and goals which emerge as the most critical will be looked at vis a vis the risk factors and risks associated with them.

2. Determine the risk factors associated with the goals. In this step, a comprehensive set of risk factors, both internal and external, that influence the initiatives and goals are determined. Risk factors may include events such as intensity of the competitive environment, fluctuations in financial markets, HR issues and changes in the political environment. Not everything can be considered, but by critically thinking through as much as possible about the types of events that could have an effect on the initiatives and goals, significantly improves that likelihood that the organization will be able to have an idea about what risks may develop.

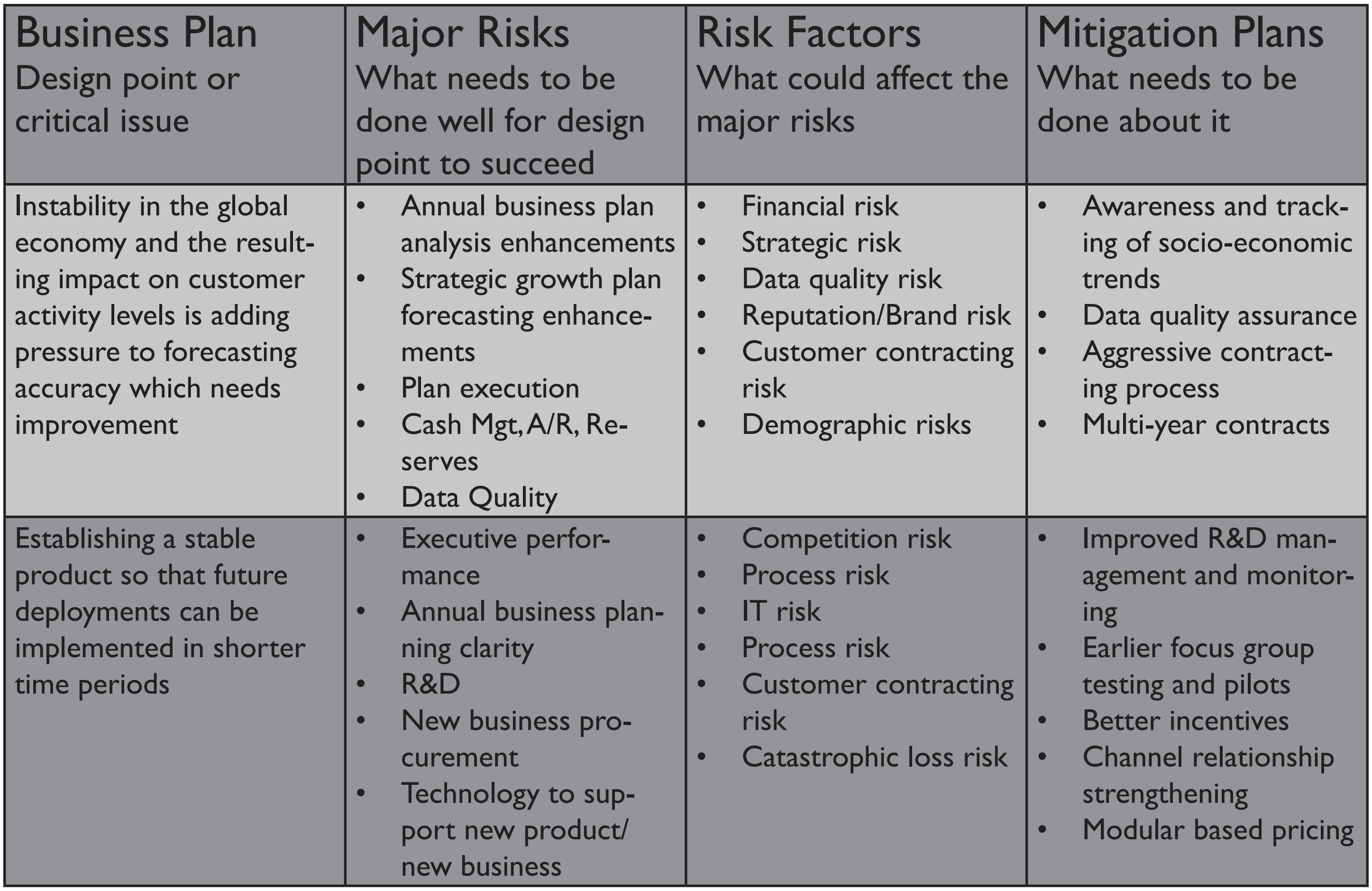
3. Identify specific risks. The organization is now in a position to determine which risks to business initiatives and goals might arise from the risk factors. Such risks should be reviewed in consideration of the full set of risk factors. How likely is the risk factor to affect the larger risk profile, and how much of an impact will it has on expected outcomes? A simple plotting of likelihood vs. impact can be developed to establish risk priorities.



4. Develop mitigation action plans. Once the major risks are clearly associated with the appropriate risk factors, mitigation plans can be established that can reduce either the likelihood or impact that risk factors might imperil the strategy. Mitigation actions can take many forms. They may include control activities but the most effective mitigation processes are those that are incorporated into daily business operations. As mentioned previously, these actions can include: 1) risk transfer, 2) doing something differently to reduce risk, 3) not doing something and eliminating the risk, 4) incorporating other protections in terms of contracts or agreements, 5) sharing risks with other partners to name just a few possibilities. Thus, ERM becomes part of the fabric of the business.

5. Produce documentation. A product that comes from this process is a document that records the most important goals in the business plan with the attendant risk factors, specific risks and risk mitigation plans. This documentation is a tool that can be used by the Board, CEO or

senior team to manage the business, monitor plan progress, review performance and so on. The following illustration reflects what a single page or screen of this documentation might look like.



Business Plan Design point or critical issue	Major Risks What needs to be done well for design point to succeed	Risk Factors What could affect the major risks	Mitigation Plans What needs to be done about it
Instability in the global economy and the resulting impact on customer activity levels is adding pressure to forecasting accuracy which needs improvement	• Annual business plan analysis enhancements • Strategic growth plan forecasting enhancements • Plan execution • Cash Mgt, A/R, Reserves • Data Quality	• Financial risk • Strategic risk • Data quality risk • Reputation/Brand risk • Customer contracting risk • Demographic risks	• Awareness and tracking of socio-economic trends • Data quality assurance • Aggressive contracting process • Multi-year contracts
Establishing a stable product so that future deployments can be implemented in shorter time periods	• Executive performance • Annual business planning clarity • R&D • New business procurement • Technology to support new product/ new business	• Competition risk • Process risk • IT risk • Process risk • Customer contracting risk • Catastrophic loss risk	• Improved R&D management and monitoring • Earlier focus group testing and pilots • Better incentives • Channel relationship strengthening • Modular based pricing

Summary

By starting the actual ERM process with the business plan, ERM easily captures top management's attention, becoming a central activity for driving the organization forward rather than a peripheral one. The types of documentation that come out of specific ERM process can be totally interwoven with planning documentation and act as a valuable tool for managing the organization and meeting goals. ■

About the Authors

Al Decker is a pricipal of Al Decker Associates, a management consulting firm specializing in enterprise risk, based in Raleigh-Durham, North Carolina. Previously, Al was the executive director of enterprise risk management for the IT firm EDS, and has extensive experience in the fields of information technology and computer & network security.

Donna Galer is n independent insurance professional based in Raleigh-Durham, North Carolina. She is currently the Chairwoman of the Spencer Educational Founcation, a nonprofit that awards scholarships to students who study risk management and insurance. Previously, she was ane xecutive vice president for Zurich Financial Services, where she was responsible at various times for a wide range of activites, including strategy, governance, human resources, investor relations, communications, shared services, business process improvement, performance management/business units and regional manager for North America.

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. It is been based on, and draws content from, of the authors' Business First™ ERM methodology.

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