CONTINUITY CENTRAL.COM
Business continuity, enterprise risk & resilience updates

The latest enterprise risk management news from around the world
Portal Publishing Ltd, PO Box 1393, Huddersfield, HD1 9TN, England

Implementing enterprise risk management

Published: Thursday, 01 March 2018 09:53

In this article by Alberto G. Alexander, some foundations will be provided for initiating the implementation of an enterprise risk management (ERM) process in an organization and the design of an ERM development model.

Introduction

Risk equates to uncertainty regarding a future outcome. Any organization is filled with uncertainty; there are few situations in which the outcome can be predicted with complete reliability. Uncertainties pose major challenges to rationality for the management of any firm.

Uncertainty is pervasive, and yet managers routinely ignore the concept of variable outcomes. Instead, they use budgets to derive a single view of the future and are then perturbed when they cannot force their firms to deliver results that precisely match the outcome predicted in the budget.

No organization can ignore risk. One has only to think of the problem that enterprises face in today's world to know that risk is something real and present:

- Natural disasters that have caused physical damage and supply chain disruption to so many corporations.
- Unexpected developments that have tarnished or ruined corporate reputations.
- Large-scale economic loss from risky financial vehicles, affecting the viability of certain corporations.

Although many risks represent a threat, it is notable that some can pose an opportunity. As an illustration, a "demographic shift could be threatening to an existing product line, but simultaneously offer opportunities for product line extensions, or a whole new line of products." (Decker, Galer, 2013).

In implementing an enterprise risk management approach to risk, a set of processes must be put into place to ensure an organization is aware of, and attends to, current and emerging risks that could alter expected outcomes. Risk is about uncertainties, and how uncertainties will affect strategic goals and objectives.

There are two widely recognized frameworks for putting ERM into practice: the COSO (Committee of Sponsoring Organizations of the Treadway Commission) Enterprise Risk

Management Integrated Framework and the ISO (International Organization for Standardization) Standard ISO 31000:2018, Risk Management-Guidelines. There are some differences between these frameworks, and each has its share of proponents. Regardless of their differences, however, they both provide meaningful structure for ERM within the organization.

This article provides practical points of guidance on the step-by-step process for implementing ERM, which fits within either of the frameworks.

Risk

Risk can mean different things to different people. The word itself evokes elements of chance, uncertainty, threat, danger, and hazard. The connotations include the possibility of loss, injury, or some other negative event.

Given these negative consequences, it would be natural to assume that one should simply minimize risks or avoid them altogether. In fact, risk managers have applied this negative definition, for many years. “Risk was simply a barrier to business objectives, and the object of risk management was to limit it” (Lam, 2017) for this reason, risk models were designed to quantify expected loss, unexpected loss, and worst-case scenarios.

In an organizational context, risk has an upside as well as a downside. Without risk, there would be no opportunity for return. A definition of risk then should recognize both its cause (a variable or uncertain factor) and its effect (positive and negative deviation from an expected outcome).

Considering these ideas, any definition of risk must always include the word uncertainty.

A simple and precise way to understand risk, in an organizational context, would be: “Variable that can deviate the performance from a specific predetermined standard”.

To understand this definition, more fully, we need to clarify two fundamental concepts, which influence a company´s overall risk profile:

- **Probability:** The more likely an event, the greater its probability and the greater the risk it presents. Events such as interest rate movements or credit card defaults are so likely that companies need to plan for them as a matter of course.

- **Severity:** This is the amount of damage that is likely to be suffered. The greater the severity, the greater the risk. Severity is the partner to probability. If we know how likely an event is to happen, and how much we are likely to suffer consequently, we have a pretty good idea of the risk we are running.

Risk is a function of probability of the occurrence of an event and its consequences.

Managing risk is at the core of any strategic, tactic or operational decision; it is about making the tactical and strategic decisions to control those risks that should be controlled and to exploit those opportunities that can be exploited.

Risk has always been present in organizations. Uncertainties pose major challenges to rationality for the management of any firm. “Technologies and environments are basic sources of uncertainty for any type of organization” (Thompson, 1967). A way to understand the performance of organizations is to perceive them as open systems. Indeterminate and faced with uncertainty, but at the same time as subject to criteria of rationality and hence needing determinateness and certainty to be able to perform according to predetermined standards. In an organization, risk is a latent event, that can become manifest at any time.

In an organizational context, risks need to be identified and mitigation actions be rapidly implemented to help the achievement of determinateness and certainty.

In organizations, how can risk be managed? In the first place, the management team should be highly cognizant of the risks to which their enterprise is subjected. At the lowest levels of effectiveness, those managers who accept the concept of risk will monitor and act on it within their processes. However, this is not especially effective, since some organizational areas that work as silos may not be addressing risk at all, and there is no consistency in the measurements and actions taken even in those situations where process managers are actively pursuing risk management. What is even worse is that usually there is no recognition of risks that occur across multiple processes. In these cases, a risk may appear to be minimal when considered separately in several organizational areas and is a serious concern when viewed in aggregate.

These situations lead us to the conclusion that the only way to effectively deal with risk is in a coordinated manner, across the entire enterprise. This concept is enterprise risk management.

Enterprise risk management

An enterprise risk management system provides a consistent methodology for locating, measuring and reporting on risks throughout an organization. It is also used to consider the impact of macroeconomic effects on an entire business; such as changes in interest rates, commodity prices, and inflation rates on the business.

Enterprise risk management considers the effects of risk across an entire enterprise. When risk is mitigated at the local level, it is entirely possible that derivatives and insurance will be used in excessive amounts, which would be reduced if local managers were aware of neutralizing transactions elsewhere in the business.

A pragmatic approach to ERM is to focus on risks that threaten the achievement of the strategy and the long-term objectives and goals.

Mr. James Lam, in his recent book "Implementing Enterprise Risk Management", (2017) gives a very precise definition of ERM, emphasizing on what it is, how it works, its main objective, and its main components.

"ERM is an integrated and continuous process for managing enterprise-wide risks, including strategic, financial, operational, compliance and reputational risks, to minimize unexpected performance variance and maximize intrinsic firm value.

This process empowers the board and management to make more informed risk/return decisions by addressing fundamental requirements with respect to governance and policy (including risk appetite) risk analytics, risk management, and monitoring and reporting".

From this definition, we could expand on the following issues:

- Enterprise risk management is a management process based on an integrated and continuous approach, including understanding the interdependencies across risks and implementing integrated strategies.
- The goal of enterprise risk management is to minimize unexpected performance variance and to maximize intrinsic firm value.
- An enterprise risk management program supports better decisions at the board and management levels.

In any company an enterprise risk management system will always remain relevant so long as it is tied to the corporate strategy, and the corporate strategy remains sound if it is supported by a solid ERM system.

The correct implementation of an enterprise risk management system implies the establishment of an ERM process, to be followed by the functional areas within an organization.

Enterprise risk management process

As was mentioned previously, an organization that practices enterprise risk management will have implemented a set of processes to be followed by the functional areas within the organization. Usually the ERM process is composed of the following phases:

- Determine
- Prearrange
- Mitigate
- Inform
- Measure.

The enterprise risk management process is depicted in figure one and a description of the most important aspects to be considered in any of these phases follows:

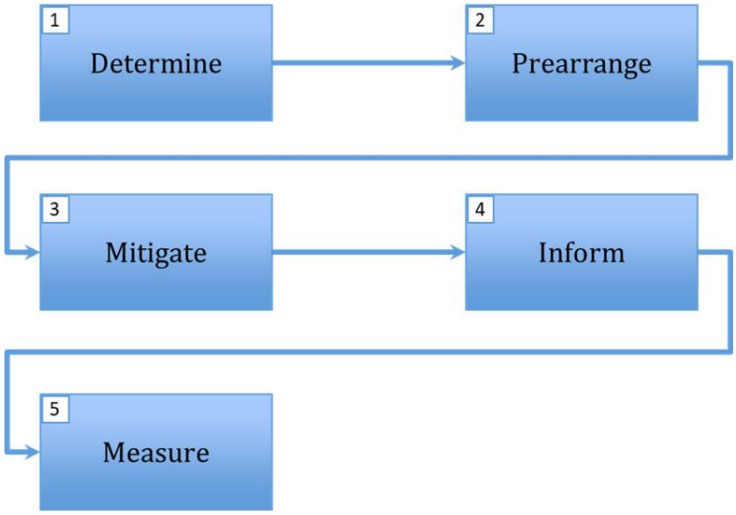

Figure one: the enterprise risk management process.

Determine

It is basically important to establish a context within which to set the identification process. That context is the corporate strategy.

Everyone involved in risk identification process needs to determine the current or emerging risks that could prevent the attainment of the goals and objectives of the strategic plan.

There are many ways to go about the 'determine' phase of the process. Typically, firms use a bottom-up approach, responding to a questionnaire, followed by mid and top management meetings where the summarized input is refined and prioritized.

Another method of identifying risk is to "hold risk profiling meetings across functions." (Decker, Galer, 2013).

Regardless of the method used in the collection of risks, those who are being asked to identify risks should be given some guidance on how to identify relevant risks. Every risk needs to be associated with its risk owner.

Prearrange

The number of risks an organization faces is immense. Any type of company does not have enough organizational slack to identify every imaginable risk. There needs to be a method to prioritize risks so that the most important ones can be identified and mitigated.

Initially the question could be: what are the most important risks that have an impact on the corporate strategy? With the risks that survive this first step, next come several other criteria such as:

- How soon is the risk likely to materialize?
- Will, the risk be repetitive?
- What is the intensity?

Prearranging risk necessarily involves measuring the likelihood of any risk and evaluating the impact or consequence of that risk occurring. This should be done with the use of scales. The most recommended scale is the "one-to-five, known also as the Likert scale" (DeVellis, 2017) which provides a combination of simplicity and some granularity and choice.

Mitigate

Risk mitigation can be defined as a systematic reduction in the extent of exposure to a risk and/or the likelihood of its occurrence.

Strategies to manage threats (uncertainties with negative consequences) typically include avoiding the threat, reducing the negative effect or probability of the threat, transferring all or part of the threat to another party, and even retaining some of or all the potential or actual consequences of a threat.

Within the ERM context, the best approach for mitigation would be to determine how the business process, underlying the risk could be enhanced or modified to address that risk.

Inform

One of the most important elements of the enterprise risk management process is informing about the risk environment and communicating the changes in that environment to enable action prior to the occurrence of a risk. The risk environment is in a constant change. These changes may alter the impact or likelihood of the risk. In all cases, change can inevitably alter the level of risk within an organization.

Informing and monitoring are continuous activities. Each organization will need to establish the system for these activities.

It is the risk owner who should be responsible for the monitoring process. The risk owner is responsible to communicating that risk to other individuals or functional areas within the firm.

Is important to remember, that risk management reports its consolidated information to its direct line management, and ultimately to the CEO and the board.

Measure

Enterprise risk management creates value at the enterprise level, but it does so because it is creating value at the functional level. The functional benefits translate into benefits of the entire organization.

It is very important to be able to measure the effectiveness of enterprise risk management, to always remember, that the end goal of ERM, is not to implement a process. The end goal is to help the enterprise achieve its goals and objectives. The extent to which ERM moves the enterprise toward this end goal is the extent to which it has been successful. This is what needs to be measured and reported to top management, with a periodical frequency.

The enterprise risk management development model

As was mentioned before, an organization that practices enterprise risk management will have implemented a set of processes to be followed by the functional areas within the organization. But to have an ERM system established and implemented in the entire organization, an ERM development program must be initiated. This program should permeate through all the components of the organizational culture. The ERM development program encompasses the ERM process.

During the rest of this article, the phases of an enterprise risk management development program will be explained.

In figure two the enterprise risk management development model is presented with its five phases.

Figure two: the enterprise risk management development model.

The main purpose of the enterprise risk management development program is to provide specific industry benchmarks of ERM practices, so companies can self-assess the degree of their enterprise risk management development program. The board members and top

management play a main role in the ERM development program. They are the main ingredients for the success of all these activities.

Let´s review the practices and benchmarks for each phase:

Setting and preparation

In phase one the organization needs to organize its resources to clarify its scope and objectives for the enterprise risk management program. During this phase, the main objectives are to identify the organization´s ERM requirements, obtaining board level and executive support. At this point, the board must be aware of its protagonist leadership role in the whole ERM program development.

It is useful to establish a cross functional taskforce to accomplish these objectives. The time for the duration of phase one is approximately 12 months. The typical activities develop in this phase are:

- Investigate about regulatory requirements and industry practices.
- Provide risk awareness programs for board members and corporate executives.
- Provide risk training for the board of directors, and managerial levels.
- Initiate training programs on how to conduct risk assessment, for managerial and supervisory levels.
- Definition of the scope, vision and overall plans for ERM.

Initial progress

The main objectives in this phase include formalizing roles and responsibilities in an enterprise risk management policy, identifying key risks through risks assessments. The five steps of the enterprise risk management process are initiated in this phase in every functional area. Risk education and awareness at different organizational levels, are developed and executed in this stage. The duration of phase two is approximately three years.

One of the most important aspects of this phase is the development of the enterprise risk management policy.

It is a good practice for the ERM policy, to include:

- An executive summary, providing the purpose, scope and objectives for ERM.
- Overall approach to risk management and appropriate guiding risk principles.
- Establishing risk tolerance levels
- Development of a risk taxonomy for commonly used terms and concepts.

Accepted method

In this phase, the firm is establishing a more timely and granular risk analysis. In this phase, the five steps of the Enterprise Risk Management Process are performing frequently. The ERM process starts permeating in the organizational culture. This phase, may take around two years. The most important activities at this stage may include:

- Developing risk databases.
- Developing key risk indicators (KRI) and establishing the policy for reporting them on a monthly basis.
- Start developing risk adjusted performance measurement methodologies.

Organizational mixture

The main goal of this phase is integrating enterprise risk management into business management and operational processes. Key objectives include quantifying the cost of risk to support pricing and risk transfer decisions, assessing business risks up front as part of business and product development. This phase could take three to five years. In this phase, the most important activities could be:

- Incorporating the cost of risk into product and relationship pricing, as well as portfolio management and risk transfer strategies.
- Developing feedback loops on risk management performance.
- Linking risk management performance and executive compensation.
- Integrating risk reviews into new business and product approval processes.

Organizational maximization

This is the most advanced phase, the enterprise risk management development program, is applied to maximize business performance and enhance relationships with key stakeholders. The main purpose of this phase is to integrate ERM into strategy development and execution.

This phase is an ongoing process and may include the following activities.

- Expanding the scope of ERM to include strategic risk.
- Full integration of ERM into strategic planning process.
- Providing risk transparency to stakeholders.
- Help customers and suppliers to manage their risks.

Conclusions

Risks may appear to be minimal when considered separately in several organizational areas but may be a serious concern when viewed in aggregate. These situations lead us to the conclusion that the only way to effectively deal with risk is in a coordinated manner, across the entire enterprise. This concept is enterprise risk management.

ERM involves so many aspects of organization´s operations, and integrates a wide variety of different types of risks; no one person is likely to have the expertise necessary to handle this entire role. In most cases, a team approach is used, with the team drawing on the skills and expertise of several different areas, including traditional risk management, financial risk management, management information systems, auditing, planning, and line operations. The use of a team approach, though, does not allow traditional risk managers to remain focused only on hazard risk. In order for the team to be effective, each area will have to understand the risks, the language, and the approach of the other areas. Also, the team leader will need to have a basic understanding of all the steps involved in the entire process and the methodology used by each area. Teams need to be trained to become skillful using the enterprise risk management process methodology.

A pragmatic approach to ERM is to focus on risks that threaten achievement of the strategy and the long-term objectives and goals.

In any company an enterprise risk management system will always remain relevant so long as it is tied to the corporate strategy, and corporate strategy remains sound if it is supported by a solid ERM.

It is very important to be able to measure the effectiveness of an enterprise risk management system, to always remember, that the end goal of ERM, is not to implement a process. The end goal is to help the enterprise achieve its goals and objectives

The board members and top management play a main role in the ERM development program. They are the main ingredients for the success of all these activities.

Ultimately what makes an ERM program work are the people. So it is very important to review how the rewarding system has been designed in the company. Are the keys performing indicators (KPIs) and the performance appraisal system reinforcing the human behavior that will make the ERM program work?

Benefits of an ERM program:

- By considering all possibilities - both positive and negative aspects of risk, management can identify new opportunities and challenges associated with current opportunities.
- Sometimes, a risk can emanate from one part of the business but have an effect on another part. As a result, management identifies and manages these entity-wide risks to sustain and improve performance.
- Enterprise risk management allows organizations to improve their ability to identify risk and establish appropriate responses, reducing surprises and related financial loss, and allowing them to profit from advantageous developments.
- Having a wealth of information on risk allows a business to assess overall resource needs and enhance resource allocation.

- Minimize the threats that could become an obstacle for the achievement of the goals and objectives of the enterprise

The author

Dr. Alberto G. Alexander holds a Ph.D from The University of Kansas, and a M.A., from Northern Michigan University. He is a MBCI, BCMS, ISMS and QMS, IRCA Lead Auditor and Approved Tutor. He is the managing director of the international consulting and managerial training firm Eficiencia Gerencial y Productividad located in Lima, Peru. . He can be contacted at alexander@eficienciagerencial.com

References

- Decker, Al. Galer, Donna. Enterprise Risk Management Straight to the Point. 2013, ERMSTTER.
- Lam, James. Implementing Enterprise Risk Management, 2017, Wiley.
- Thompson, James. Organizations in Action, 1967 Mc Graw Hill
- DeVellis, Robert. Scale Development, Theory and Applications, SAGE, 2017.