Enterprise Project Governance[1]

How to Manage Projects Successfully Across the Organization

Dealing with Uncertainty

By Paul Dinsmore & Luiz Rocha

The Development of Risk Management

Before the early 1980s, risk was relatively new to those outside the insurance industry. At that time companies were able to transfer certain risks to insurance companies. These transferred risks related to natural catastrophes, accidents, human error or fraud. Later, companies began to look more closely at financial risks, like exchange rates, commodity prices, interest rates and stock prices. This was the beginning of financial risk management as a formal system.

A major drive towards more formalized approaches to risk management, corporate governance and internal controls resulted from the high-profile collapses of major corporations since the late 1990s. These scandals found executives testifying that they were unaware of unethical activities carried on by their companies. This prompted new regulatory environments such as Sarbanes-Oxley (SOX) in the US, the Combined Code on Corporate Governance in the UK and the Basel II Accord for the banking sector, all with a strong focus on internal controls and making company executives responsible for establishing, evaluating and monitoring the effectiveness of their company's internal control structure. The most widely accepted definition of internal control was developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO): "a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: effectiveness and efficiency of operations; reliability of financial reporting; compliance with applicable laws and regulations."

The most contentious aspect of SOX is Section 404, which requires management to produce an annual internal control report which must affirm the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting. The report must also contain an assessment of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

[1] *This series includes articles by Paul Dinsmore and Luiz Rocha, authors of the book Enterprise Project Governance, published by AMACOM in the USA in 2012. The articles are extracts and summaries of key topics from their book, providing information and guidance on one of the most important aspects of portfolio, program and project management today – governance. For information about the book, go to http://www.amacombooks.org/book.cfm?isbn=9780814417461.*

Internal controls are fundamental to the successful operation and day-to-day running of a business and assist the company in achieving their business objectives. The scope of internal controls is very broad. It encompasses all controls incorporated into the strategic, governance and management processes, covering the company's entire range of activities and operations, and not just those directly related to financial operations and reporting. The scope is not confined to those aspects of a business that could broadly be defined as compliance matters, but extends also to the performance aspects.

In the same way internal control is a key aspect of corporate governance, risk management is a vital element of internal control since bad risk management may affect the internal controls in all organizational areas. Identifying risks and creating systems and safeguards to ameliorate them is one way to create a sound internal control framework. As a result, internal controls depend on effective risk management to guarantee quality performance and compliance for organizations to achieve their business objectives. Because CEOs and CFOs are obliged to make public statements attesting to the effectiveness of internal control, a framework is required based on objective criteria and subject to measurement.

As the field of risk management expanded, proposals were formed towards creating a corporate culture able to hurdle the risks associated with rapidly changing business environments. The concept was tagged Enterprise Risk Management (ERM). The overarching principle of ERM is that it must produce value for the organization producing a net effect that is more than the cost of risk management and risk controls.

危機

For risk to be seen as adding value to an organization, a view broader than the conventional meaning of "danger" is required. The word risk is depicted in Chinese by two characters that give insight to a more holistic meaning. The first character signifies "threat" and the other "opportunity". In this sense, risk can be seen as having a down side and also an upside, where indeed the threatening component exists, yet opportunities also dwell. Enterprise risk management effectively boils down to avoiding unnecessary exposure that might endanger meeting projected goals, and at the same time, staying alert for opportunities to add value.

Risk Management Maturity Continuum

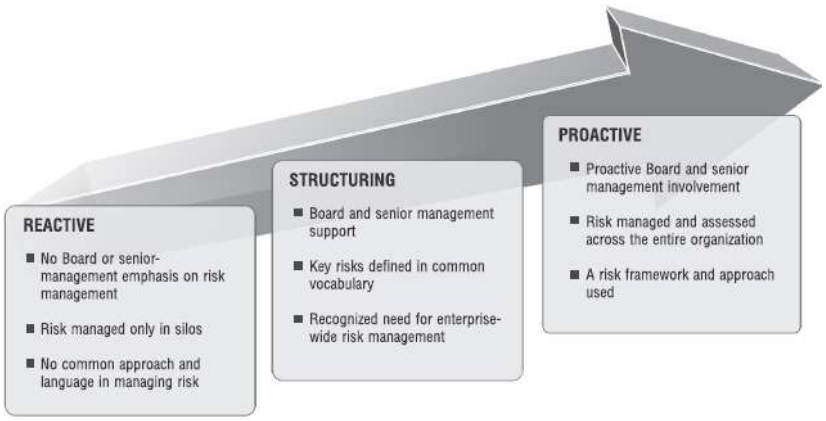
Risk management takes on different forms in different organizations. The responsibility may rest solely with a part-time professional or, at another extreme, require a full-fledged department to deal with an array of multi-billion dollar issues. At Mars Corporation, a world-wide multi-billion dollar corporations noted for chocolate bars, an Enterprise Risk Management (ERM) program was approved by the board and implemented over a four-year period. A series of implementation workshops were

conducted throughout the organization to help create a solid base for reaping benefits from risk management. Once established the basic risk culture, Mars began to integrate ERM into other managerial pillars such as strategic planning and performance management. The risk management framework was also used to interact with the business units for identifying and mitigating strategic and operational risks at that level.

The Mars ERM team takes a proactive stance in working with leaders throughout the organization by conducting annual workshops that provide opportunity for open exchange of views about potential risks and how to deal with them. Here risks of all natures are examined, including strategic, operational and those related to portfolios, programs and projects.

Overall risk management in organizations evolves over time and is impacted by a learning process as shown in the exhibit below. First, organizations begin reacting to risks and are managed in silos with no common language to communicate across the company. Once organizations recognize the need for an integrated approach, a common vocabulary begins and key organizational risks are identified. More and more the organization understands the need for structuring.

Finally, risk management becomes part of the enterprise strategic thinking. The adoption of an overall risk management policy helps create awareness and commitment and keeps senior management focused on high level risks that will affect results and the organizations' capacity to meet its objectives. Nevertheless, there is a wide perception that the current state of maturity is low. A 2010 COSO survey highlighted that the state of ERM appears immature with 60 percent of respondents saying that their risk tracking is mostly informal and applied in silos and that there is a notable level of dissatisfaction with how organizations are currently overseeing enterprise-wide risks.



The Risk Management Maturity Continuum

ISO 31000 and ERM

The International Organization for Standardization (ISO) non-certifiable standard 31000, Risk Management: Principles and Guidelines, published in 2009 with the participation of 30 countries, seek to answer differing views on risk and risk management. The standard supports a simple way of thinking about risk and risk management and is designed to resolve the many inconsistencies and ambiguities that exist between differing approaches and definitions.

Every organization has its own unique risk footprint and its own risk management challenges and the aim is to establish a consistent framework that can be integrated across various industries and regions and adopted by any organization – including public, private, not-for-profit and government organizations in order to benefit all organizations confronting the always problematic challenges of managing risk.

ISO 31000 defines risk as the **effect of uncertainty on objectives**. Risk is the consequence of an organization setting and pursuing objectives against an uncertain environment. The uncertainty is driven by internal, external factors that may cause the organization to fail to achieve its objectives. Striving towards business goals always carries an element of risk and uncertainty and it is the effective management of that risk which enables meeting the established goals. This definition is totally aligned with the top management aims of driving the organization to a desired point in the future.

The ISO standard is built around three fundamental pillars: Principles, Framework and Processes. The principles position risk management as fundamental in the success of the organization rather than a wearisome burden. As such, risk management must be considered to create and protect value and an integral part of the organization's processes and decision making. As a critical discipline, each decision-maker is accountable for risk management, including the identification, analysis and evaluation of any risks.

The standard also states that to be successful, risk management should function within a risk management framework which provides the foundations and organizational arrangements that will embed it throughout the organization at all levels. The risk management framework is the management system that defines and describes how risk management will permeate the organization. Once commitment is established, using a systematic, structured and timely approach makes risk management a continual and active process and not a once a year exercise that can be left on the shelf to gather dust.

By simplifying complex concepts and coupling the framework with the process and principles ISO 31000 is likely to subsume all the existing risk management standards by providing a platform for developing effective management of risk no matter where a company's operations are located. Some of the benefits presented by the norm as resulting from managing risk include: full integration in the organization's governance structure (in which EPG is included); improved governance; increased likelihood of

achieving objectives; improved identification of opportunities and threats; compliance with relevant legal and regulatory environment and improve controls.

ERM and EPG

Managing risk in an integrated way can mean everything from using financial instruments to managing specific financial exposures, from effectively responding to rapid changes in the organizational environment to reacting to natural disasters and political instability. Within this wider understanding of integrated risk management the ability to tackle the risks involved across the strategy/execution gap is mandatory as discussed in previous chapters.

The EPG realm addresses the strategy/execution gap by considering risk management as part of portfolio, program and project management processes already covered by well-known standards. But one could appropriately question that risks are in the focus of ERM. In reality, EPG benefits from the overall structure for ERM while EPG supports ERM with their well established processes to identify, analyze and mitigate risks. There is no redundancy but integration if adequately aligned.

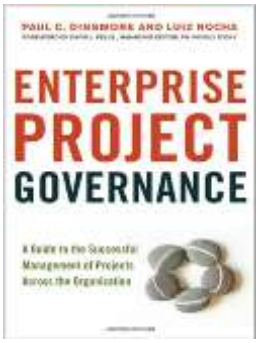
Effective implementation of integrated risk management can produce a number of benefits to the organization which are not available from the typical limited-scope of analyzing only risk processes without considering the broader context of the permanent organization.

This is the only way of providing useful information to decision-makers when the environment is uncertain, to support the best possible decisions at all levels, creating space to manage uncertainty in advance, with planned responses to known risks, and minimizing threats and maximizing opportunities, and so increasing the likelihood of achieving strategic objectives.

Conclusions

Risk management can be applied to an entire organization and has earned increasing attention at executive levels. It is also part of portfolio, program and project management and as such an integral part of enterprise project governance. Yet, although perhaps less dramatic, major organizations also face possible disasters when risk management is lacking in their portfolio of projects. For this reason risk management is a component of EPG and a link with ERM must be established. In reality care should be taken to guarantee an integration and articulation between ERM, EPG, strategic planning and auditing.

When risk management is implemented and maintained accordingly the ground is prepared for the development of a risk-mature culture within the organization, recognizing that risk exists in all levels of the enterprise, but that risk can and should be managed proactively in order to deliver benefits. After all, the greatest risk of all is to take no risk at all.



Enterprise Project Governance describes proven techniques for dealing with simultaneous initiatives and ensuring that programs and projects align with the priorities, resources, and strategies of the organization - and ultimately create value. Containing examples and case studies, the book provides readers with practical methods for incorporating enterprise project governance into their organization's culture, synchronizing it with corporate governance, and maximizing efficiency and results across departments.

Whether one's view is from the boardroom, the executive suite, the project management office, or the project trenches, this is an important guide for anyone managing multiple projects. For more about the book, go to http://www.amacombooks.org/book.cfm?isbn=9780814417461.

About the Authors

Paul C. Dinsmore

Paul Dinsmore is President of Dinsmore Associates, and a highly respected specialist in project management and organizational change. A certified project management professional (PMP), he has received the Distinguished Contribution Award and Fellow Awards from the Project Management Institute (PMI®). He regularly consults and speaks in North America, South America, Europe and Africa. Paul is the author and / or editor of numerous articles and 20 books, including the *AMA Handbook of Project Management*. Mr. Dinsmore resides in Rio de Janeiro, Brazil.

Luiz Rocha

Luiz Rocha has 35+ years of experience in the industry and business consulting. Luiz worked with Andersen Consulting and Delloite in the USA and Europe when he had the opportunity to manage multi-cultural and geographically dispersed projects in Latin America, North America and Europe. In Brazil he worked with Dinsmore Associates and Petrobras. Luiz is an engineer by background, MSc. in industrial engineering from UFRJ – Brazil, PMP-PMI and IPMA certifications. He is also a published author with two previous books, *Business Metamorphosis,* in Brazil, and *Mount Athos, a Journey of Self-Discovery,* in the USA. Luiz can be contacted at luiz.rocha@dinsmore.com.br.