Chapter 7

Enterprise Risk Management to Drive Operations Performances

Giulio Di Gravio, Francesco Costantino and Massimo Tronci

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/54442

1. Introduction

Global competition characterizes the market of the new millennium where uncertainty and volatility are the main elements affecting the decision making process of managers that need to determine scenarios, define strategies, plan interventions and investments, develop projects and execute operations (figure 1).

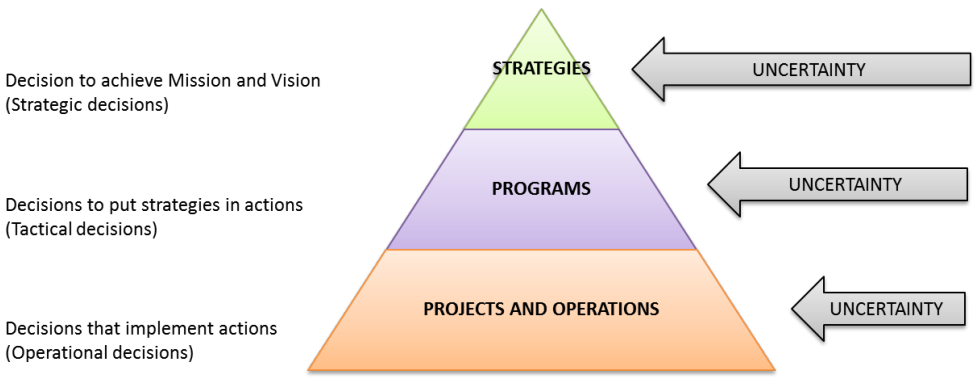

Figure 1. Decision hierarchy

Risks have been always part of entrepreneurships but a growing attention to the issues related to Risk Management is nowadays spreading. Along with the financial scandals in the affairs

of some major corporations, the high degree of dynamism and the evolutions of markets need organizations to rapidly adapt their business models to changes, whether economic, political, regulatory, technological or social [1].

In particular, managerial trends of business disintegration, decentralization and outsourcing, pushed organizations towards practices of information sharing, coordination and partnership. The difficulties that generally arise during the implementation of these practices underline the impact that critical risk factors can have on corporate governance. Operations, at any level, are highly affected in their performance by uncertainty, reducing their efficiency and effectiveness while losing control on the evolution of the value chain.

Studies on risk management have to be extended, involving not only internal processes of companies but considering also the relationship and the level of integration of supply chain partners. This can be viewed as a strategic issue of operations management to enable interventions of research, development and innovation.

In a vulnerable economy, where the attention to quality and efficiency through cost reduction is a source of frequent perturbations, an eventual error in understanding the sensibility of the operations to continuous changes can seriously and irreparably compromise the capability of fitting customers' requirements.

Managers need to have personal skills and operational tools to ensure that risk management strategies can be suitably implemented and integrated in the production and logistics business environment. In order to face internal and external uncertainty, take advantage of it and exploit opportunities, it is necessary to identify, analyze and evaluate operational risks through standard methodologies that help to:

- classify the different types of risks;
- identify risks in scope;
- assess risks;
- identify possible interventions and relative priorities;
- select, plan and implement interventions, managing actions and collecting feedbacks.

While studies and standards on risk management for health and safety, environment or security of information defined a well-known and universally recognized state of the art, corporate and operational risk management already needs a systematic approach and a common view. The main contributions in these fields are the reference models issued by international bodies [2-5].

Starting from the most advanced international experiences, in this chapter some principles are defined and developed in a framework that, depending on the maturity level of organizations, may help to adequately support their achievements and drive operations performance.

http://dx.doi.org/10.5772/54442

2. Corporate governance and risk management

Over the years, the attention to the basic tenets of corporate governance has radically increased.

In response to the requirements of supporting business leaders in managing organizations and in protecting the various stakeholders towards the evolution of the political, economic and social environment, guide lines and reference models in the field of corporate governance have been issued.

Within this body of rules, risk management plays a main role. It relates directly to the recognition of the strategic connotations of corporate governance as the means to achieve business targets, according to the rights and expectations of stakeholders.

Since the mid-nineties onwards, the themes of risk management and corporate governance are strictly intertwined and almost coincident: the systematic management of risks has become a synonym of a "healthy" management of the business. At the same time, the techniques of risk analysis, historically associated with assessing financial risks, have been revised or replaced by methods that pervade the organization in depth. Along with the use of specific and complex control models (i.e. the experience of the Code of Conduct of the Italian Stock Exchange), responsibility for risk management is placed at the level of senior management. In some countries, such as Germany, Australia and New Zealand, these indications reached the level of compulsory requirements as national legislation asks all companies to have an operational risk management system.

From the above, the close link between corporate governance and risk management is absolutely clear. It has to be considered not only as an operational practice but rather as an essential component of decision making, based on the continuous development of definition systems and, therefore, of the top management responsibility.

The management of the company risk profile requires the knowledge of:

- the risk system affecting the enterprise;
- the nature and intensity of the different types of risks;
- the probability of occurrence of each risk and its expected impact;
- the mitigation strategies of the different types of risks.

To ensure that the approved, deliberated and planned risk management strategies are executed in an effective and efficient way, the company's top management shall periodically review and, if necessary, implement corrective and/or preventive action with regard to:

- reliability of existing systems for the identification and assessment of risks;
- effectiveness of internal control systems to monitor risks and their possible evolution.

Corporate governance is thus to be seen as the strategic platform on which the tactical and operational system of risk & control acts, i.e. the set of processes, tools and resources at all levels of the organization to ensure the achievement of corporate objectives. On these argu-

ments, it is appropriate to consider that the application of a system based on the principles of risk & control governance allows the creation of a virtuous circle of performances that has a positive impact on the environment inside and outside the company, beyond regulatory requirements.

Management has the responsibility to plan, organize and direct initiatives to ensure the achievement of company goals, in terms of:

- definition of business and government targets;
- formulation of strategies to reach business and government targets;
- effective and efficient use of the resources of the organization;
- relevance and reliability of financial and operational reporting;
- protection of company assets;
- compliance with laws, regulations, contracts and corporate ethical standards;
- protection of ethical and social values.

The management acts through a regular review of its objectives, changes in processes according to changes in the internal and external environment, promoting and maintaining a business-oriented culture and a climate.

3. Risk classification

Uncertain events can have both a positive and a negative effect: on the one hand, in fact, they are a threat to the achievement of business objectives, on the other hand can become a significant source of opportunities for companies able to understand, anticipate and manage them. According to [6], *risks* are *"events with negative impacts that can harm the creation of business value or erode the existing one*" while *opportunities* are *"events with positive impact that may offset negative impacts"*. The opportunities are chances that an event will occur and positively affect the achievement of objectives, contributing thus to the creation of value or preserving the existing one. Management needs to assess the opportunities, reconsidering its strategies and processes of setting goals and developing new plans to catch benefits derived from them.

An inherent risk can so be defined as "the possibility that an event occurs and have a negative impact on the achievement of objectives" while the control can be defined as "any means used by management to increase the likelihood that the business objectives set are achieved", mitigating the risks in an appropriate manner. In this context, a hazard is a "potential source of risk" while a residual risk is the "risk that still remains after mitigations".

Along with these definitions, it is possible to organize the different types of risks in different classes and their possible combinations. In Table 1 a first example of classification is shown, based on two characteristics that relate the origin and generation of the risk (organizational perimeter) with the possibilities of intervention (controllability of risk).

http://dx.doi.org/10.5772/54442

		Controllability		
Organization		*Controllable*	*Partially controllable*	*Uncontrollable*
	Internal	Quality and cost of products	Environmental impacts	Incidents and accidents
	External	Technological progress	Demand variation	Natural disasters

Table 1. Example of risk classification by perimeter

Further classifications can also be taken from the already mentioned risk management models, where the descriptive categories are represented as a function of different objectives and decision-making levels (Table 2).

Model	Dimension	Classes
Risk Management Standard [3]	Level of interaction (internal and external)	- Strategic risks (partner and market) - Financial risks (economic-financial cycle) - Operational risks (process) - Potential risks (social and territorial environment)
Strategy Survival Guide [7]	Decisional level	- External risks (PESTLE - Political, Economic, Socio-cultural, Technological, Legal/regulatory, Environmental) - Operational risks (delivery, capacity and capability, performance) - Change risks (change programs, new projects, new policies)
FIRM Risk Scorecard [8]	Area of impact	- Infrastructural risks - Financial risks - Market risks - Reputational risks
Enterprise Risk Management [4]	Area of impact	- Strategic risks - Operational risks - Reporting risks - Compliance risks

Table 2. Example of risk classification by target

Developing the classification to an extended level and considering all the sources of uncertainty that affects business targets, vulnerability of organizations can be assessed on five different areas (Table 3).

Risk Category	Risk factors
Demand (Customers)	- Number and size of customers - Changes in number and frequency of orders - Changes to orders - Seasonal and promotional effects - Forecasting - Warehouses and inventory - Level of innovation and competition - Life cycle of the product - Timing and mode of payment - Retention rate
Offer (Suppliers)	- Number and size of suppliers - Level of quality and performance - Level of flexibility and elasticity - Duration and variability of lead time - Length and mode of transfers - Forecasting and planning - Just-in-Time or Lean approaches - Cost efficiency - Price levels - Outsourcing - Internationalization - Disruption
Processes (Organization)	- Flexibility of production-distribution systems - Variability in process management - Variability in process performance - Level of productivity - Capacity - Handling - Operational and functional failures - Redundancy of backup systems (quantity and quality) - Profit margins - Technological standards - Technological innovation of product and process - Product customization
Network and collaboration (Relations)	- Trust and interdependence among partners - Level of collaboration - Design and development of relations - Level of integration - Level of service - Opportunism and information asymmetry in transactions - Bargaining power

http://dx.doi.org/10.5772/54442

Risk Category	Risk factors
	- Strategic objectives and mission
	- Corporate cultures
	- Business Logic
	- Relationship and stakeholder engagement
	- Social and administrative responsibility
	- Availability and reliability of information systems
	- Intellectual property
Environment (Externalities)	- Regulations
	- Policies
	- Laws
	- Taxes
	- Currency
	- Strikes
	- Natural events
	- Social events (i.e. terrorism)

Table 3. Risk classification by organization

4. Enterprise risk management for strategic planning

The competitiveness of an organization depends on its ability to create value for its stakeholders. The management maximizes the value when objectives and strategies are formulated in order to achieve an optimal balance between growth, profitability and associated risks, using resources in an efficient and effective way. These statements are the basic philosophy of "risk management business". As seen, all businesses face uncertain events and the challenge of management is to determine the amount of uncertainty acceptable to create value. The uncertainty is both a risk and an opportunity and can potentially reduce or increase the value of the company.

The Enterprise Risk Management (ERM) is the set of processes that deals with the risks and opportunities that have an impact on the creation or preservation of value. ERM is put in place by the Board of Administration, the management and other professionals in an organization to formulate strategies designed to identify potential events that may affect the business, to manage risk within the limits of acceptable risk and to provide reasonable assurance regarding the achievement of business targets. It is an ongoing and pervasive process that involves the whole organization, acted by people of different roles at all levels and throughout the corporate structure, both on its specific assets and on the company as a whole.

This definition is intentionally broad and includes key concepts, critical to understand how companies must manage risk, and provides the basic criteria to apply in all organizations, whatever their nature. The ERM enables to effectively deal with uncertainty, enhancing the company's ability to generate value through the following actions:

- *the alignment of strategy at acceptable risk:* management establishes the level of acceptable risks in evaluating strategies, setting objectives and developing mechanisms to manage the associated risks;
- *the improvement of the response to identified risks:* ERM needs a rigorous methodology to identify and select the most appropriate among several alternatives of responses to risks (avoid, reduce, share, accept the risk);
- *the reduction of contingencies and resulting losses*: companies, increasing their ability to identify potential events, assess the risks and formulate responses, reducing the frequency of unexpected events as well as the subsequent costs and losses.
- *the identification and management of multiple and correlated risks*: every business needs to face an high number of risks affecting different areas and the ERM facilitates the formulation of a unique response to clusters of risks and associated impacts;
- *the identification of opportunities:* through the analysis of all possible events, management is able to proactively identify and seize the opportunities that emerge;
- *the improvement of capital expenditure:* the acquisition of reliable information on risks allows management to effectively assess the overall financial needs, improving the allocation of resources.

These characteristics help management to achieve performance targets without wasting resources. Furthermore, it ensures the effectiveness of reporting in compliance with laws and regulations, so to prevent damages to corporate reputation and relative consequences. Summarizing, the ERM supports organizations to accomplish their goals while avoiding pitfalls and unexpected path.

5. The risk management process

The risk management process consists of a series of logical steps for analyzing, in a systematic way, the hazards, the dangers and the associated risks that may arise in the management of an organization. The goal is realized in giving maximum sustainable value to any activity, through a continuous and gradual process that moves from the definition of a strategy along its implementation. By understanding all potential positive and negative factors that affect the system, it is possible to increase the probability of success and reduce the level of uncertainty.

In particular, risk management protects and supports the requirements of the organization in its relationship with stakeholders through:

- a methodological framework that allows a consistent and controlled development of activities;
- the improvement of the decision-making process, creating priorities by really understanding the natural and exceptional variability of activities and their positive or negative effects;
- the contribution to a more efficient use and allocation of resources;

http://dx.doi.org/10.5772/54442

- the protection and enhancement of corporate assets and image;
- the development and support to the people and to their knowledge base.

Figure 2 represents a process of risk management in its different stages of development that are detailed in the following sections.

5.1. Risk assessment

Risk assessment is a sequence of various activities aimed at identifying and evaluate the set of risks that the organization has to face. The international literature offers several techniques of modeling and decision-making [9-10] that can become part of the analysis.

The results of risk assessment can be summed up in two outputs that address the following stages of treatment and control:

- the risk profile;
- the risk appetite.

The risk profile represents the level of overall exposure of the organization, defining in a complete way the complexity of the risks to be managed and their ranking, according to their entity and significance. A segmentation for entities (areas, functions, people, sites) or decisional levels and the actual measures of treatment and control complete the profile. This takes to the expression of the:

- *gross profile:* the level of exposure to the events without any measure of treatment;
- *net profile:* the level of exposure, according to the measures of treatment in place (if effective or not);
- *net future profile:* the level of exposure surveyed after all the measures of treatment are implemented.

The definition of the risk appetite is a key outcome of the assessment process: on the one hand it is appropriate to draft it before the risk identification (where the level of accuracy of analysis can also depend on the risk appetite itself), on the other it is absolutely necessary to fix it before taking any decision about the treatment.

In any case, the risk appetite presents two different dimensions according to the scope of analysis:

- *threat*: the threshold level of exposure considered acceptable by the organization and justifiable in terms of costs or other performance;
- *opportunity*: what the organization is willing to risk to achieve the benefits in analysis, compared with all the losses eventually arising from a failure.

The so defined risk appetite can be adjusted through the delegation of responsibilities, strengthening the capability of taking decisions at different levels according to cost dynamics.

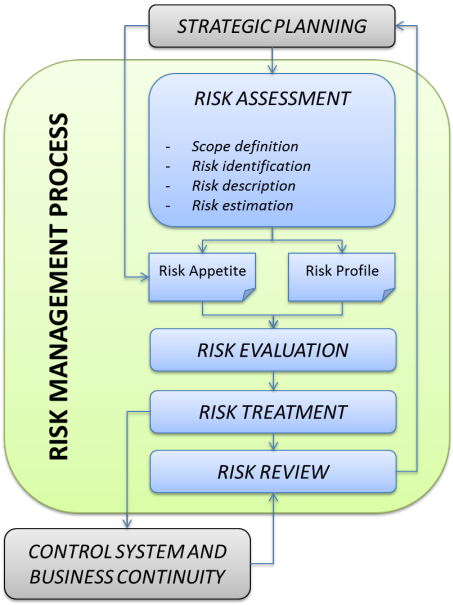

Figure 2. Risk Management process

5.1.1. Scope definition

The target of this stage is the identification of assets and people exposed to the risks and the identification of factors that determine the risks themselves. The definition of the scope has a critical importance in order to evaluate internal and external influences on the organization.

As this analysis requires requires a thorough knowledge of the environmental components (business, market, political, social and cultural issues), it has to be developed for all the decision-making levels (strategic, tactical and operational) and for all the stakeholders. Furthermore, the relationships with the output of the strategic planning have to be determined as the relevance of a risk and the priorities of interventions can be identified only with reference to the targets to uncertainty, while the eventual impact can vary widely according to a proper assignment and commitment of resources.

Despite this stage is found to be of fundamental importance for the effectiveness of the others, in particular for the identification of risks, it is too often executed with an inappropriate level of attention or it is not developed at all.

5.1.2. Risk identification

The identification of risks allows to acquire knowledge on possible future events, trying to measure the level of exposure of the organization. The target is to identify all the significant

http://dx.doi.org/10.5772/54442

source of uncertainty in order to describe and proactively manage different scenarios. The identification is the first step to define the *risk profile* and the *risk appetite* of the organization.

This activity has to be repeated continuously and can be divided into two distinct stages:

- initial identification of risks: to be developed for organizations without a systematic approach to risk management. It is required to gather information on hazards and their possible evolutions;
- ongoing identification of risks: to update the risk profile of an organization and its relations, taking into account the generation of new risks or modifications to the already identified ones.

All the process mapping techniques are extremely useful to associate and connect risks with activities (Figure 3). The level of detail is determined by the necessity of identifying the specific impact associated with risks, of assigning responsibility of management and defining the subsequent actions to ensure control.

This can be developed with the support of external consultants or through a self-assessment which, if conducted with adequate methodological tools, provides a better awareness of the profile and an upgrade of the management system.

Among the others, the most common and widely used (successfully tested in other fields as for marketing and quality management) are:

- techniques of data collection and statistical analysis;
- techniques of problem finding and problem solving;
- SWOT analysis and Field Force;
- benchmarking with competitors or best in class.

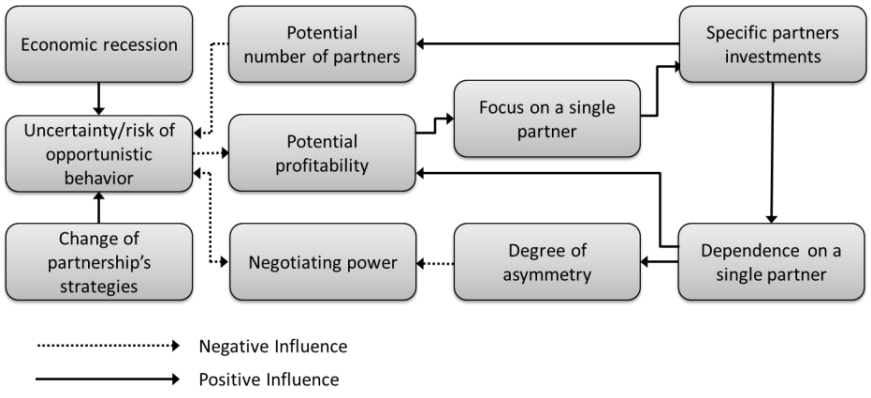

Figure 3. Example of risk identification for collaboration risks

5.1.3. Risk description

The results of identification should be developed in an appropriate stage of description by means of specific information support systems (i.e. Risk Register, table 4). Depending on the scope, the documentary support can assume different forms to improve the sharing of information and increase efficiency of management. Whatever the solution adopted for the description, this has to be dynamically completed with data coming from the different stages of the risk management process and updated according to changes of internal and external context. Inheriting the best practices already in use for environmental and safety management systems, when the risks are in any way related to regulations (i.e. Sarban Oaxley's act), a Compliance Register has to be associated to the Risk Register to ensure the conformity to requirements.

5.1.4. Risk estimation

The risk assessment has to end up with the association of a qualitative or quantitative measure of any risk, in terms of technical, economic or financial intensity. The choice of the methodology is related to the level of details required by the comparison among risk profile and risk appetite and to the availability of data and information. The metrics can refer to:

- probability of occurrence and magnitude of the effects and impacts;
- value at risk or vulnerability, which is the possible value of benefits or threats in relation to the characteristics of the organization.

The estimation of risk can be performed using different qualitative, quantitative or mixed criteria each with a different level of detail and reliability of the results. While the first are characterized by a strong subjectivity that only a high level of experience can compensate, the second need harmonization and conversion of the scales and of the values found. The choice is also related to the desired output of the stage, typically a hierarchical ordering of the risks identified (e.g. some types of exposures and tolerability are defined by regulations, especially for safety and environment). Examples of simple evaluation criteria, according to the already mentioned reference model, are shown in table 4, 5 and 6.

Identification code	ID to associate and create links among information
Category	According to the classification adopted
Organizational level	Corporate, business unit, site, process or activities involved
Related target	Relation to the strategic planning and decisional level
Stakeholders	Involvement of the different stakeholders
Regulation	Relation to compulsory (laws or directives) or voluntary (procedures) requirements
Description	Extended description of the event and its possible evolutions (hazard)
Causes	First, second and third level causes (direct or indirect)

http://dx.doi.org/10.5772/54442

Consequences	Description of impacts (direct or indirect)
Emergency	Potential emergency related to the risk and associate plans of recovery
Inherent risk	Combination of the probability (or frequency) of the event and the impact or relevance of the effects
Risk appetite	Threshold level of tolerance of the specific risk
Treatment	Extended description of the mitigations
Residual risk	Estimation of the risk after the of mitigation
Control	Extended description of the control
Risk owner	Responsibility of the risk and related activities
Control owner	Responsibility of the control and related activities

Table 4. Risk register

High	- financial impact on the organization probably higher than xxx € - notable impact on strategies or operations of the organization - notable involvement of the stakeholders
Medium	- financial impact on the organization probably among yyy € and xxx € - reasonable impact on strategies or operations of the organization - reasonable involvement of the stakeholders
Low	- financial impact on the organization probably lower than yyy € - limited impact on strategies or operations of the organization - limited involvement of the stakeholders

Table 5. Impacts of threats and opportunities [3]

Value	Indicator	Description
High (Probable)	Probable every year or in more than 25% of cases	- possible happening of the event in the period of analysis, with many repetitions - it happened recently
Medium (Possible)	Probable in 10 years or in less than 25% of cases	- possible happening of the event in the period of analysis, with some repetitions - difficulties in forecasting and controllability - data on past events exist
Low (Remote)	Improbable in 10 years or in less than 2% of cases	- mostly likely it never happens - it never happened

Table 6. Probability of the event: threats [3]

Value	Indicator	Description
High (Probable)	Probable advantages in the year or in more than 75% of cases	- clear opportunity with reasonable certainty - to act in the short period with the actual processes
Medium (Possible)	Reasonable advantages in the year or between 75% and 25% of cases	- achievable opportunity that requires an accurate management - opportunity beyond the programs
Low (Remote)	Possible advantages in the midterm or in less than 25% of cases	- possible opportunity that has to be deeply examined - opportunity with low probability of success according to the actual resources involved

Table 7. Probability of the event: opportunities [3]

5.2. Risk evaluation

The evaluation of risks provides a judgment concerning the acceptability or the need of mitigations, according to the comparison between the risk profile and the risk appetite. The stage is a decision-making process in which, if the risk is acceptable, the assessment can be terminated, otherwise it goes on to next stage of treatment and management. To verify the acceptability after the interventions, the results of the mitigations have to be iteratively compared to the expected targets. At this stage it is possible to use, with adaptation when necessary, methods and techniques widely tested in safety management:

- *Event Tree Analysis (ETA) and Fault Tree Analysis (FTA):* analysis of the cause-effect tree of the risk profile. The top event (an event that is at the end of the shaft) is usually a cause of loss of value in the organization, related to exclusionary or concurrent events of a lower-level type;
- *Failure Modes Effects Analysis (FMEA) and Failure Modes Effects and Criticality Analysis (FMECA)*: FMEA is a technique that allows a qualitative analysis of a system, decomposing the problem in a hierarchy of functions up to a determined level of detail. For each of the constituents, possible "failure modes" (adverse events) are identified and actions to eliminate or reduce the effects can be considered. FMECA adds a quantitative assessment of the criticalities: for each mode, an index is calculated as the combination of the occurrence of the event, the severity of its effects and the detectability of the symptoms;
- *Hazard and Operability (HAZOP) analysis*: qualitative methodology that has both deductive (search for causes) and inductive (consequence analysis) aspects. The method seeks for the risks and operational problems that degrade system performances and then find solutions to the problems identified;
- *Multi-criteria decision tools (i.e. Analytic Hierarchy Process and Analytic Network Process)*: decision support techniques for solving complex problems in which both qualitative and quantitative aspects have to be considered. Through a hierarchical or network modeling, the definition of a ranking of the critical aspects of the problem is enabled. Multi-criteria decision

http://dx.doi.org/10.5772/54442

tools give an effective support mainly where the consequences of an event can be both positive and negative, applying cost-benefit analysis.

5.3. Risk treatment

Treatment of risks must be determined after a first evaluation and comparison of the risk profile and the risk appetite of the organization. The actions arising from this decision-making stage can be classified according to the following scheme:

- *terminate*: remove, dispose or outsource, where possible, the factors that can cause the risk. It can take the organization to refuse opportunities if the value at risk is higher than the risk appetite;
- *treat:* develop measures of mitigation in order to intervene on the values of significance of the risk, reducing the probability of occurrence (prevention), the potential impacts of the effects (protection) or determining actions of restoring (recovery) after damages are occurred. Passing from prevention to protection and recovery, the capability of controlling risks tends to decrease, while increasing the exposure of the organization;
- *tolerate*: accept the risk profile as compatible with the risk appetite, in relation to the resource involved;
- *transfer*: transfer the impacts to third parties through, for example, insurances or risk sharing actions. Possible uncertain effects are converted in certain payments;
- *neutralize:* balance two or more risk, for example increasing the number of unit exposed, so that they can cancel each other;
- *take the opportunity:* when developing actions of treatment, opportunities of positive impacts can be identified and explored.

5.4. Risk review

The key target of the review stage is to monitor the changes in the risk profile and in the risk appetite of the organization and to provide assurance to all stakeholders that the risk management process is appropriate to the context, effectively and efficiently implemented.

The frequency of the review should be determined depending on the characteristics of the risk management system, to execute:

- *a review of the risks*, to verify the evolution of already existing risks and the arise of new risks, assessing their entity;
- *a review of the risk management process*, to ensure that all activities are under control and to detect changes in the structure of the process.

6. The control system

The conceptual path that characterizes this approach to risk management is strictly related to the existence of an indissoluble connection between risks and controls. Most current control systems recognize the risk as part of the corporate governance that has to be:

- continuous, integrating control in the decision-making processes;
- pervasive, spreading the risk management at all decisional levels;
- formalized, through the use of clear and shared methodologies;
- structured, through the adoption of suitable organizational solutions.

The control system traditionally represents a reactive approach in response to adverse events, fragmented in different areas and occasional frequencies. From a standard dimension, generally limited to financial risks or internal audit, it has to evolve towards a proactive continuous process, results-oriented and with widespread responsibility. The challenge for management is to determine a sustainable amount of uncertainty to create value in relation to the resources assigned, facing a costs and benefits trade-off where the marginal cost of control is not greater than the benefit obtained.

The main components of the control system can be summarized as follows:

- *control environment*: it is the base of the whole system of controls as it determines the sensitivity level of management and staff on the execution of processes. The adoption and dissemination of codes of ethics and values, policies and management style, the definition of a clear organizational structure and responsibilities (including specific bodies of internal control), the development of professional skills of human resources are the elements that constitute this environment;
- *control activities*: it is the operational component of the control system, configured as a set of initiatives and procedures to be executed, both on process and interfaces, to reduce business risks to a reasonable level, ensuring the achievement of the targets;
- information and communication: a structured information system at all levels enables the control on processes, recomposing flows managed by different subsystems and applications that need to be integrated. Adequate information, synthetic and timely, must be provided to allow the execution of activities, taking responsibilities and ensuring monitoring;
- *monitoring*: it is the continuous supervision and periodic evaluation of the performances of the control system. The scope and techniques of monitoring depend on the results of the risk assessment and on the effectiveness of the procedures in order to ensure that the controls are in place to efficiently reduce the risks.

http://dx.doi.org/10.5772/54442

7. The business continuity

But how can organizations deal with those types of risks generally unknown and not predictable? The answer comes from a different kind of strategic vision that is not only based on the analysis of identified risks but looks at the possible modes of disruption of processes regardless of the cause. For example, once defined the logistics distribution as a key factor for the success of the business, you can evaluate how to recover any link regardless of the specific reasons of interruption.

The Business Continuity Management is an approach generally used in case of possible serious consequences related to crisis or emergency [11-13]: an organization that evaluates the effects of damage to a warehouse caused by a sudden storm or defines actions following the failure of a partner is performing risk management; when it arranges structured actions related to the unavailability of a warehouse or a provider moves up to the level of Business Continuity Management and its main features:

- analysis and identification of the elements of the organization that may be subject to interruption, unavailability and related effects;
- definition of action plans and programs to be implemented when an element is missing, to ensure the continuity of material and information flows or recover as quickly as possible;
- monitoring of processes to anticipate possible crises or to start emergency plans;
- establishment of systematic test of recovery plans;
- once recovered, structured analysis of events to evaluate the success of the initiatives, the efficiency of the plans and their revision.

The Business Continuity Management accompanies organizations during disaster recovery of unexpected risks, particularly rare and with high magnitudes of the effects, where the operations must be carried out with the utmost speed and effectiveness. Events such as the earthquake in Kobe (Japan) in 1995, that caused more than 6,400 deaths, 100,000 demolished buildings, closed the major ports of the country for two months, having a general impact on industries for more than 100 billion dollars, can easily be presented for examples of disasters. At the same time, also much smaller events can be recognized as a disaster for small and medium-sized enterprises, such as the loss of a key customer, a huge credit not collected, a wrong industrial initiative, a failure of the production system or the breakdown of a relationship with a partner.on dollars, the other much smaller events also can be recognized as a disaster for small and medium-sized enterprises, such as the loss of a key customer, a huge credit not collected, a wrong industrial initiative, a system failure or breakdown of a relationship with a partner. In the same way, any loss related to a failure of an infrastructure can generate adverse effects as well as an incorrect definition of strategic processes or the indiscriminate and uncoordinated introduction of new methods such as just-in-time: the majority of negative events come from managerial mistakes that could be avoided rather than from the effects of real and unexpected emergencies.

A recovery plan must therefore meet the following requirements:

- ensure the physical integrity of employees, customers, visitors and in any case all subjects interacting with current activities;
- protect as much as possible facilities and resources to ensure a rapid recovery;
- implement procedures to restore a minimum level of service, while reducing the impact on the organization;
- work with partners to redefine the appropriate services: once reorganized the internal activities, it is necessary to seek outside to assess the effects and consequences of actions taken;
- return all processes to performance standard in time and at reasonable cost: the speed with which the repairs must be carried out is balanced with the associated costs.

8. Conclusions

The main advantages that companies could obtain from Enterprise Risk Management were deeply investigated in the sections above. Anyway, this novel approach could present some difficulties, common to many businesses, related to the absence of a culture of strategic planning aimed at prevention rather than response, to a general lack of professionals and of appropriate tools capable to really integrate processes. But while complexity is becoming a part of the corporate governance system, absorbing a great amount of time and resources, the need for competitiveness requires a specific attention to performances and results. A new attitude of organizations towards risk-sensitive areas, able to ensure the coordination among all its components, helps to transform the management of risk from a cost factor to an added value. This business view, allows, with a little effort, to reduce the overall risk of the company and helps the dialogue among business functions and with the stakeholders.

Author details

Giulio Di Gravio*, Francesco Costantino and Massimo Tronci

*Address all correspondence to: giulio.digravio@uniroma1.it

Department of Mechanical and Aerospace Engineering, University of Rome "La Sapienza", Italy

References

[1] Minahan T.A. The Supply Risk Benchmark Report. Aberdeen Group; 2005.

[2] UK HM Treasury. Orange book management of risk – principles and concepts. 2004.

http://dx.doi.org/10.5772/54442

[3] Association of Insurance and Risk Managers (AIRMIC), GB Institute of Risk Management (IRM), ALARM National Forum for Risk Management. A Risk Management Standard. 2002

[4] AU Committee of Sponsoring Organizations of the Treadway Commission. Enterprise Risk Management – Integrated Framework. 2004.

[5] European Foundation for Quality Management. EFQM framework for risk management. EFQM; 2005.

[6] ISO Guide 73:2009 - Risk Management - Vocabulary. ISO; 2009

[7] UK Prime Minister's Strategy Unit. Strategy survival guide. 2004.

[8] Information Security Forum. Fundamental Information Risk Management (FIRM). ISF; 2000.

[9] ISO 31000:2009. Risk management - Principles and guidelines. ISO; 2009

[10] ISO/IEC 31010:2009. Risk Management - Risk Assessment Techniques. ISO; 2009

[11] British Standard Institute. PAS56: Guide to Business Continuity Management. BSI; 2006.

[12] Chartered Management Institute. Business Continuity Management. CMI; 2005.

[13] Department of Trade and Industry. Information Security: Understanding Business Continuity Management. Stationery Office; 2006.