NORMS AND INTERNATIONAL STANDARDS RELATED TO REDUCE RISK MANAGEMENT: A LITERATURE REVIEW

César Fuentes*, Edmundo R. Lizarzaburu**, Edgar Vivanco***

Abstract

The current work aims to develop a revision of the literature within the main concepts in the international rules and standards related to risk management in companies. By this way, there will be an analysis of issues such as the COSO - ERM model, an introduction to the ISO 27000 and 31000 standards; and the Project Management according to PMI targeted at risk management.

Keywords: COSO, ISO 27001, ISO 3100, PMI, Risk Management, Projects, Information Security, Risk Evaluation

**Corresponding Author School of Business, Esan University, Alonso de Molina 1652, Monterrico Chico, Surco, Lima, Peru*
E-mail: cfuentes@esan.edu.pe
***School of Business, Esan University, Alonso de Molina 1652, Monterrico Chico, Surco, Lima, Peru*
Email: elizarzaburu@esan.edu.pe
****Email: edgar.vivanco@usil.pe*

1. Introduction

In recent years there has been a growing concern about risk management and the need of having a solid reference frame to identify, evaluate and manage risk effectively has been identified (Flaherty, 2004).

Therein, several scholars such as Robert I. Mesh, Bob A. Hedges, Clifford W. Smith and Rene M. Stulz have focused on Enterprise Risk Management (ERM) (Liebenberg & Hoyt, 2003). This provides a process by which the company articulates all the features of risk management (Pagach & Warr, 2007) and as a consequence, that company improves the management of the volatility of prices of their actions and their profits, as well as an improvement in the capacity of supervising the portfolio risks (Beasley et al, 2006 & Warr, 2008).

On the other side, the information of the company is one of the most important assets they own and has such a value for the organization that several mechanisms must be developed to ensure a suitable protection (Alvares & Garcia, 2007). That is why, the information security which main purpose or objective is to keep the continuity of the organizational processes that support assets, reduce the global cost of performance of such processes and losses of the appointed resources for their operation (Sema Group, 2006), have become so important. For that reason, it is necessary that the responsible people of the information security in their organizations realize the role they perform and contrast risks their assets may go under. Risk evaluation, analysis and treatment allow take the risk level of the assets of the organization to acceptable values (Pessolani, 2007).

Finally, the globalization has hurried the rhythm of innovation and technological development creating a constant transformation in the market and a huge growth of the demand of products and services which has promoted great development of the knowledge management and the studies of project management (Karapetyan & Otieno, 2011).

2. Risk Management

Risk Management is an essential step in the economic and financial assessment. It is a strict and documented approach in all levels of development of analyzed events which demands information of all areas of interest.

Risk Management has become a central issue in the financial management[80] in the last years. Risk is not a new concept. From the beginning and the middle 20th Century several authors showed interest to that issue such as Markowitz[81] in 1952 and 1959. The seminal work of Knight (1921) clearly points out a distinction between risk and uncertainty, being the first measurable and feasible to delimit by historic experience, sample data or a subjective or Bayesian evaluation of risks. On the other hand, uncertainty is not measurable for the viewpoint of the author and most risk appraisers.

[80] Das, S. *Risk Management.* Wiley Finance, 2006.
[81] Markowitz, Harry, (1959). *Portfolio Selection, Efficient Diversification of Investments,* John Wiley and Sons, Inc

Risk Management must take into account the dynamic nature of projects. Not only do we consider the negative consequences of an event but also the positive consequences. Cooper et al (2005) states this need saying that "only the management of the negative perception of risks is, in fact, to omit half the responsibilities of the projects manager". Jaafari (2001) and Ward and Chapman (2003) support this statement of showing the importance of considering the risks and opportunities during the process of risk analysis.

Furthermore, the Project Management Institute (PMI) and the Association for Project Management (APM), show the following definitions:

- **Risk:** "An uncertain event or condition that, if happens, produces a positive or negative effect in the objectives of a project" (PMI, 2004).
- **Risk:** "An uncertain event or group of circumstances that, if happens, produces an effect in the achievement of the objectives of the Project" (APM, 1997).

Ward and Chapman go further and suggest an approach called the uncertainty of management that considers the positive and negative consequences of uncertainty (Chapman and Ward, 2003). They state the word "risk" has a negative connotation which complicates the exploration of opportunities in the identification of risks and the analysis process. In this point, authors clearly deviate from the paradigm appointed by Knight (1921), the Risk Management focuses on the management and identification of all the sources of uncertainty, the formation of threats and opportunities.

"The complete management of risks or the Complete Management of Risks (CMR) has shown great development in the recent years as a consequence of the need to know and manage the levels of risk to which a company is exposed during the performance of the strategy and the achievement of goals due to the process of globalization mostly which has extended considerably the range of opportunities as well as risk to which companies face"[82].

The word "risk" comes from the Italian word risicare that means "to defy, to challenge, to face, to dare". In the New Spanish Dictionary, it is Latin etymologically defined as "Danger, test, attempt, to expose to danger, to put somebody in danger, to pose a danger, to face danger" (De Miguel and el Marqués de Morante, 1887, p. 211). "According to Philippe Jorion, risk can be defined as the volatility of unexpected financial flows generally produced from the values of assets and liabilities".

There is not only one accepted definition of risk at a long term. The Oxford English Dictionary defines risk as "the possibility of something unpleasant to happen" and the origins of the term are referred to 17th Century to Risco, Italian words, riscare and richiare (Hay-Gibson, 2009).

Giddens suggests that a root of the word risk comes from a Portuguese word that means "to dare" (Althaus, 2005; Hay-Gibson, 2009). As well as the definition of a record, risk is defined in different ways in different contexts and from different epistemological perspectives. As a matter of fact, Hay-Gibson (2009) defines risk as, "(…) The possibility of an event to happen in terms of its risk, generally with a negative connotation". He points out that risk is a "trans-disciplinary" issue.

The fact that risk is transverse to different activities makes the interpretation of the term more complex. The scope of risks of Information Technology defines risk as any event that affects the company, a case that happens with the frequency and uncertain extent and that creates problems in the achievement of goals and strategic objectives. (ISACA, 2010).

In other words, the perception of individuals of levels of risk and the real objective of the feasibility of an event neither match the regulations or definitions of risk nor the sequence defined by the academy. Even though the definitions vary, it is likely to obtain certain common ideas associated to the concept of risk. Risk is often typified as an unequal event related to specific consequences (ISO /IEC, 2009). In fact, the references to the risks are frequently associated to the mixture of the probability of the event and the consequences of such event (ISO / IEC, 2009). From the side of the computers security it is impossible to extend the additional concept of a menace combined with a vulnerability that a risk situation produces. (Harris, 2010)

Risk management has been followed by several authors (Bernstein, 1996; Barlow, 1993; Covello and Mumpower, 1985; Thompson, et al, 2005; Althaus, 2005; Hay-Gibson, 2009). These ones suggest that it is an old policy and the place and time that Duranti (1989) and others have traced at the beginning of this Management – is Tigris Region and Euphrates Valley. It started at about 3200 BC. Covello and Mumpower described the way in Asipu (risk early Managers) as consultants for uncertain or difficult decisions.

Others suggest that the origins at the beginning of the Risk Management are still under discussion (Hay-Gibson, 2009). The history of Risk Management takes into account that the information provided by Diderot and Voltaire promoted the beginning of the risk management as modernly known and at the same time produced the modern concept of historic files (Covello and Mumpower, 1985; Posner, 1984).

ISO 31000 standard defines Risk Management as "Coordinated activities to lead and control an organization with respect to risk" (ISO / IEC, 2009), whereas the Genetic Advisers compare risk management as the process to advise clients in the

[82] AS / NZS Rule 4360:1999, Australian Standard of Risks Management

way of managing risk related to the genetic tendency to particular disorders (Austin, 2010). It is concluded by studies of Helsinky University of Technology (Porthin, 2004) in relation to the number and variety of definitions of risk management is that the idea of risk and its management is only referred to decisions made from high management which purpose is to identify, evaluate and reduce risks. Furthermore, the rule points out: "… Different types of organizations of all sizes face internal and external factors and influence that create uncertainty if they achieve their objectives or not.

All the activities of an organization imply certain risk. Organizations manage their risk by identification and analysis and then assessing if risk should be modified by the treatment of risk with the purpose of satisfying risk criteria. By this process, organizations communicate and advise implied parties, monitor and review risk and controls that are modifying it with the purpose of guaranteeing that no additional treatment of risk is needed. This rule describes this systematic and logical process in detail …"[83]

Covello and Mumpower (2006) find that generally the risk analysis methodologies include the following common elements: (i) the mathematical notion of probability (It will perform either qualitatively or quantitatively), (ii) a process of establishing causation and risk identification, and (iii) the processes and strategies to reduce these risks. Risk Management ISO standards outlines a number of activities, including evaluation, treatment, monitoring and reviewing risk, and documentation of their management process (ISO / IEC, 2009). With slight variations of context, activities now form the basis of the standard practice of Risk Management through a number of different areas. So, "from fields as diverse as document management is genetic counseling, analysis activities related to risk management and strategies to face risk appear to be relatively uniform".[84]

3. Literature Review

3.1. COSO – ERM Model

The Treadway Commission *(Committee of Sponsoring Organizations of the Treadway Commission – COSO)* was formed in 1985, in response to the inefficiency of internal controls. For example, errors and irregularities by deficiencies in Information Technology, collusion and negligence of people, and other operational failure events. (Ernst & Young, 2011).

The result was published on the internal control integrated framework to help organizations assess and improve their internal control systems. This framework has been incorporated into policies and regulations within organizations seeking to improve control of their activities to improve the achievement of its objectives.

Thus, it was verified the need of a reference frame for Risk Management which provides among other things: principles and key concepts and a common language with clear guidance. COSO believes that this integrated framework of Enterprise Risk Management (ERM) meets this need, and expects to be widely accepted by companies and other organizations and, in fact by all other groups of interest (COSO, 2004).

In 1992 the publishing of the integrated Reference Frame redefines the internal control, developing a conceptual framework with tools to evaluate and improve controls. Then, in 1996 a comprehensive method that describes 89 principles of best practices for effective risk management within a financial institution is provided, collected in the Generally Accepted Risk Principles (GARP: Generally Accepted Risk Principles[85]).

In the field of audits and internal control, the Sarbanes-Oxley Law of 2002 (US Government Printing Office) aims to improve protection to shareholders through a series of measures, very demanding, affecting the different agents involved in public markets businesses. Thus, the Law influences significantly, among others, on the Boards of Directors, on the directors of these companies, on investment banks, on financial analysts, and also, on a major way, on the activity and regulation of accounts auditors. The duties and responsibilities of each of those involved in the companies listed in the American market (Díaz, 2005).

In terms of the evolution of the Internal Control Model, ERM began to be widely discussed and developed initially by large financial institutions. COSO began with the creation of an ERM framework by Financial Intelligence units to provide a solid base on which companies can improve corporate governance and deliver greater value to shareholders (Bowling & Rieger, 2005).

Even though ERM does not want to replace the internal control framework, it seeks to incorporate so as to provide a more solid and wide focus. However, ERM is not just limited to the internal control requirements but can evolve into a process of comprehensive risk management (COSO, 2004).

Despite the valuable contribution that the emerging practice of ERM makes the model, there are also some limitations. For example, it cannot establish a standard for identifying the effectiveness of the ERM. Its definition of risk focuses on the internal field and does not take into account the opportunities and external threats. Adopting an approach of command and control does not take into

[83] ISO 91000:2009 Rule

[84] Lemieux, V. (2010). The record-risk nexus: exploring the relationship between records and risk,. Record Management Journal .20(2), 199-216.

[85] http://riskinstitute.ch/00011593.htm

account the shared management of threats with external factors and social implications of ERM.

As a result of that, the bias of not considering the opportunities becomes systemic. It is now apparent, since the ERM has been institutionalized within the rules, practice and expected standards of good management (Williamson, 2007).

Treadway Comission (1992) defines ERM as: *"A process affected by the board of directors, management and staff of an institution, applied in the development of the strategy throughout the organization designed to identify potential events that may affect the entity and manage the risk to find within the risk profile established to provide reasonable assurance of achieving the objectives of the organization."*

From the above definition it is concluded that ERM is a continuous process that is transverse to an entity. Shenkir and Walker (2006) suggest that executives should be willing to commit, because they are responsible to protect, create and increase shareholders value. It also involves fundamental concepts of risk management in companies, providing a basis for its application within organizations, industries and sectors. The ERM is focused directly on achieving the goals set by a particular entity and provides a basis for defining effective enterprise risk management.

According to the previously mentioned, it is identified that the widespread application of ERM has been established for two primary reasons:

- **Sarbanes-Oxley Law (2002):** It seeks to reach a higher level than the application of this Law, in which public financial instructions apply, in particular section 404 of the Law. *Therefore, increased emphasis on corporate governance and related to the rising costs of compliance are driving business leaders to consider if the enterprise-wide approach to risk management will generate greater value from their investments in SOA compliance. They see the ERM as the next step in a logical progression for the development of its risk management activities. In its fullness, the ERM has the potential to reduce compliance costs, improve operational performance, improve corporate governance and deliver greater value for shareholders.* (Wagner & Lee, 2006).
- **Publication of the new COSO framework:** The model describes the key components and principles of risk management for organizations regardless of size. The ERM has a broad view of risk, an important step forward compared with the fragmentation of risk management in many organizations. It focuses on the causes and effects that can keep companies achieve their strategic business objectives.

3.1.1. Achievement of Objectives Approach in the Model

In the context of the mission or vision of an institution, the administration has established strategic objectives, selects the strategy and sets targets through the company hierarchy. This framework of enterprise risk management is aimed at achieving the objectives of the organization, established in four categories: strategic, operational, finance and compliance with governing laws and regulations. This categorization of objectives focuses on different aspects of enterprise risk management. These different but overlapping categories (a particular target can belong to more than one category) address the needs of the organization and may be the direct responsibility of different executives. The categorization also allows distinguish between what can be expected from each category of objectives (Ernst & Young, 2011). Because the objectives regarding the reliability of the information and compliance with laws and regulations are within the control of the organization, it is expected that corporate risk management can provide reasonable assurance for the achievement of these objectives (Root, 1998).

3.1.2. Components of the Model

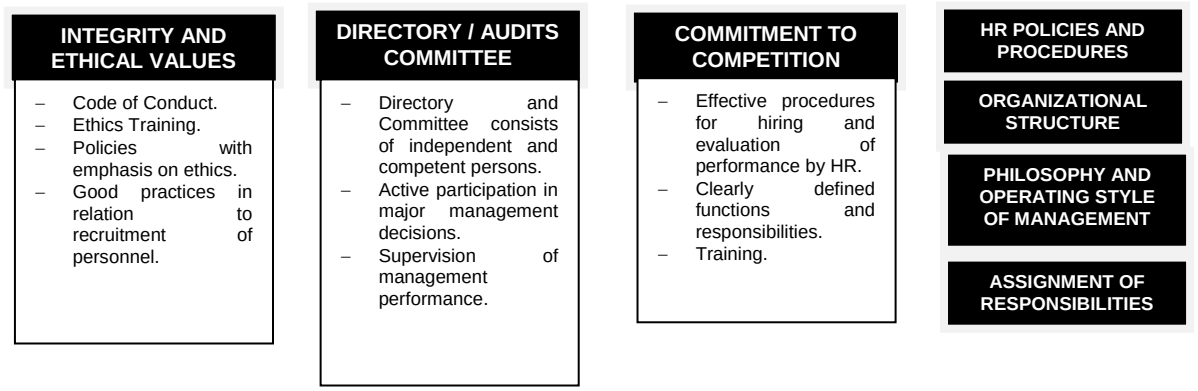
COSO-ERM model consists of 8 interrelated elements, which are derived from the way management runs a business and are integrated with the management process (Moeller, 2007). It has been proposed a three-dimensional model that provides criteria for assessing internal controls with three objectives: effectiveness and efficiency of operations, reliability of financial information and compliance with laws and regulations.

These components are[86]:

- **Internal Environment:** The internal environment includes the style of the organization, and seeks to influence the awareness of people regarding to risk, including risk management philosophy, integrity and ethical values, and the environment in which they operate. (Ernst & Young, 2011).

[86] Gupta, Parveen P., COSO 1992 Control Framework and Management Reporting on Internal Control: Survey and Analysis of Implementation Practices (June 10, 2009).

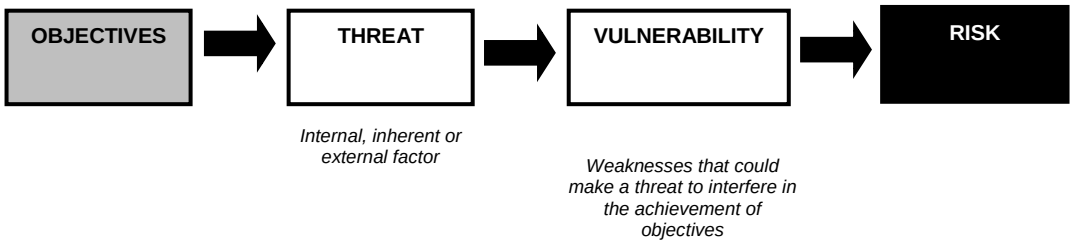
Chart 1. COSO - ERM: INTERNAL ENVIRONMENT INDICATORS



Source: Ernst & Young 2011

- **Stating Objectives:** ERM ensures that management has implemented a process to set goals and that the selected targets support and match the goals of the organization and are consistent with their risk profile (Ernst & Young, 2011).

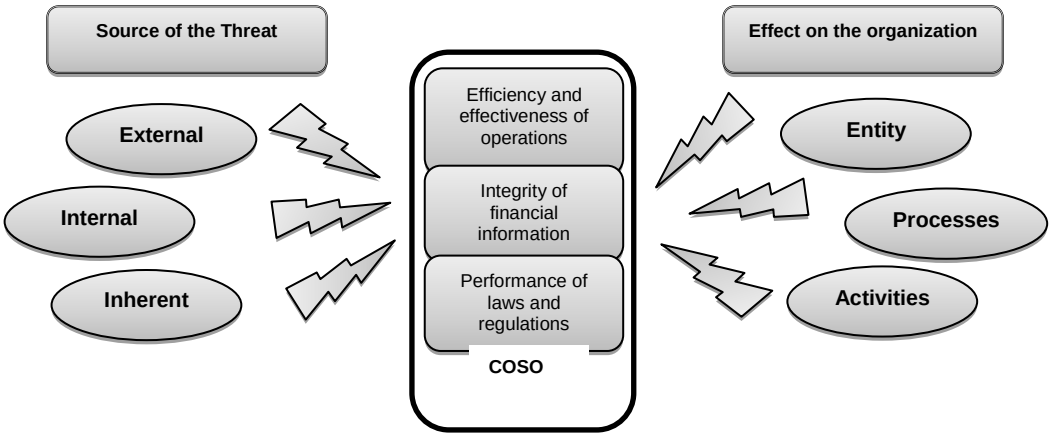
Chart 2. COSO - ERM: relationship between objects, threats and vulnerabilities



Source: Ernst & Young 2011

- **Identification of Events:** Events (internal and external) that affect the achievement of the objectives of the organization must be identified, making a difference between risks and opportunities. (Ernst & Young, 2011).

Chart 3. COSO - ERM: risk categorization



Source: Ernst & Young 2011

The organization should identify internal and external risks that could prevent business goals from achieving.

Table 1. COSO - ERM: internal and external risks

CATEGORY	DESCRIPTION
EXTERNAL	Risk that come from environmental conditions and which cannot influence the organization.
INTERNAL	Risk that come from decisions made by the organization and use of internal and external resources.
INHERENT	Risk inherent in the business, are usually independent of the sector or type of organization.

Source: Ernst & Young 2011

The risks may vary according to the effect they have on certain levels of the organization.

Table 2. COSO - ERM: HAZARD LEVELS OF ORGANIZATION

CATEGORY	DESCRIPTION
ENTITY	Broader risks that affect all the organization. Top management assumes responsibility for remedial.
PROCESS	Specific risks of a particular process. The solution is often left to those responsible for the processes.
ACTIVITY	Risks that come from the performance of particular tasks or activities.

Source: Ernst & Young 2011

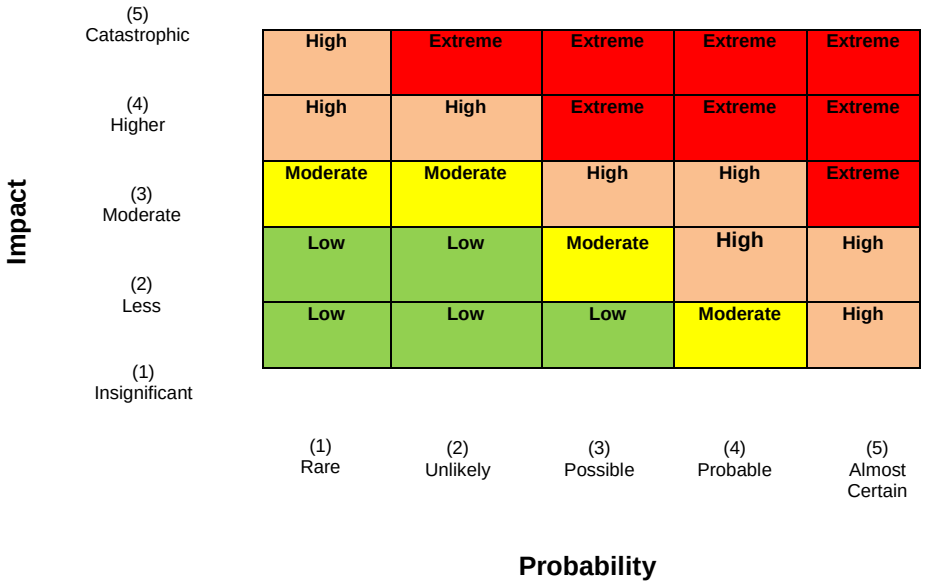
- **Risk Evaluation:** Risk evaluation is the process of analysis and prioritization of risks relevant to achieving the objectives of the entity and to determine an appropriate response. (Ernst & Young, 2011).

Risks are analyzed, taking into account the probability of occurrence and impact, which will determine their treatment:

- **Severity of Impact:** Level of financial exposure of the company at risk or amount of financial loss that could be generated if a risk event occurs.
- **Probability of occurrence:** Degree of possibility that the risk event occurs over a period of time.

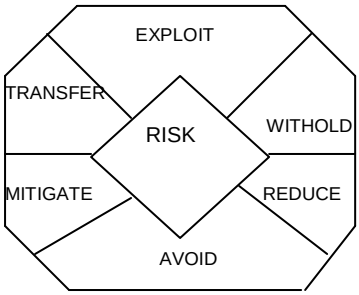
- **Answering to Risks:** Management selects risk responses: avoid, accept, reduce or share risk, developing a series of actions to adapt risks to the risk profile of the entity. (Ernst & Young, 2011).
- **Control Activities:** Policies and procedures are set up and implemented to help ensure that risk responses are effectively carried out. (Ernst & Young, 2011). These measures seek to mitigate and manage risk so that it is likely that a process achieves its objectives.

Chart 4. COSO - ERM: RISK EVALUATION LEVEL



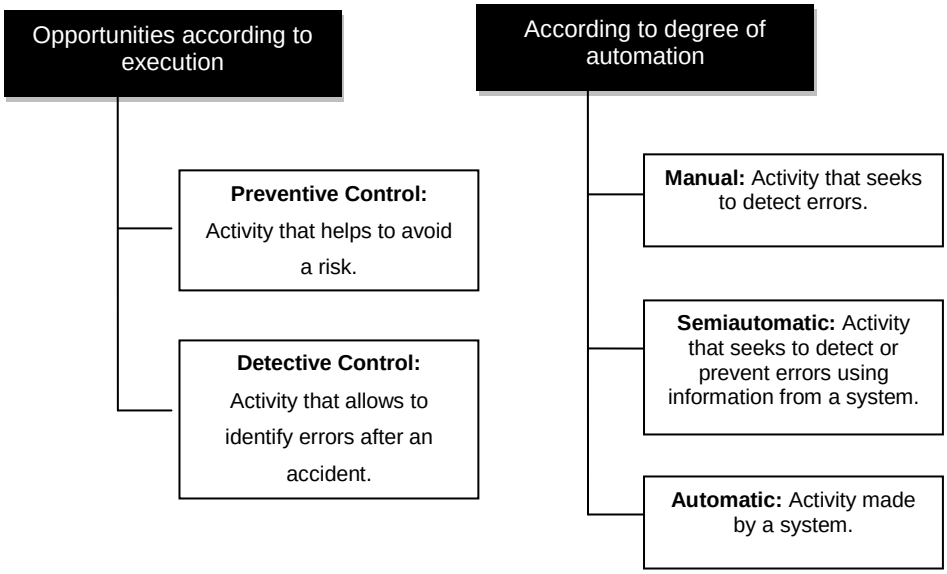
Source: Ernst & Young 2011

Chart 5. COSO - ERM: STRATEGIES FOR THE TREATMENT OF RISKS



Source: Ernst & Young 2011

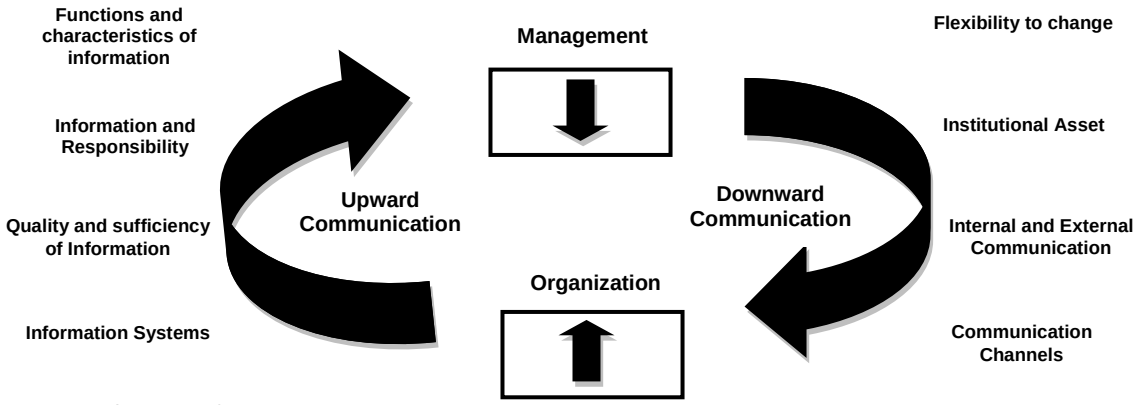
Chart 6. COSO - ERM: TYPES OF CONTROL



Source: Ernst & Young 2011

- **Information and Communication:** Relevant information is identified, stored and communicated in the way and terms that allow people to carry out their responsibilities. (Ernst & Young, 2011)

Chart 7. COSO - ERM: INFORMATION AND COMMUNICATION SYSTEMS



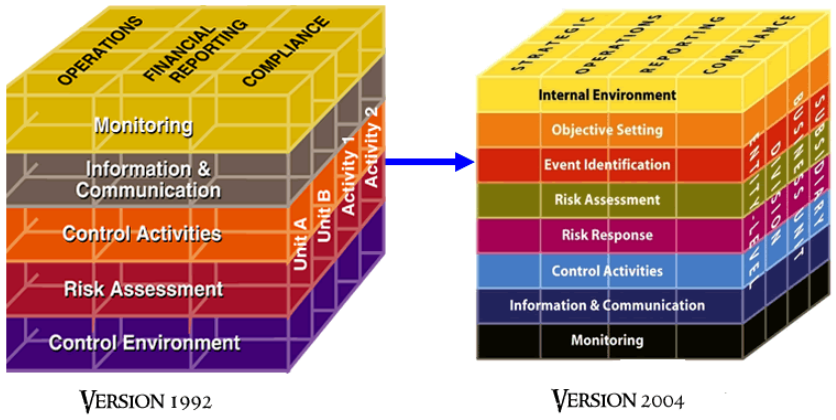
Source: Ernst & Young 2011

- **Supervision:** Because management of risk is a multi-directional and interactive process where almost any component may have and has influence over another, supervision is carried out through activities of management in progress, separate assessment, or both aspects in order to obtain reasonable security that the objectives will be achieved as well as those related to internal control. (Ernst & Young, 2011)

3.1.3. Relation to the objectives and components

There is a direct link between the objectives the entity wants to achieve and the components of the management of corporate risk that represent what is missing to obtain to achieve them. The link is represented by a cube-shaped, three-dimensional array

Graph 8. COSO: EVOLUTION (1992-2004)



Source: COSO 2004

The four categories of objectives: strategy, operations, information and performance are represented by vertical supports. The eight components are represented by flat rows and the units of the entity by the third dimension of the cube. This graph shows the capacity of focusing on the whole management of corporate risk of an entity or by category of objectives, component, unit or any sub-group wanted, as well. (COSO, 2004)

3.2. Information Security and Risk Management

As business is developed rapidly and industries seek to organize efforts related to risk management, market participants expect that the corporate programs of Risk Management provide with more detailed data for their analysis and support a better

decision-making which involves new standards for Risk Management[87] and information security directly.

Thus, organizations realize that it is necessary to work under the guidelines of ISO rules. For example, ISO 9000 develops quality issues, whereas ISO 14000 Rule has an approach within management and respect to environment (Yates & Murphy, 2007). Furthermore, there is another series of ISO rules that has started to play a more important role in the scope of risk management.

The three rules that implement management systems have many issues in common (Brewer & Nash, 2005). Firstly, they are based on Deming Cycle (1950) that states the requirements and processes that allow a company to set up, implement, control, manage and keep efficient management, whether quality, environment, or information security (Humphreys, 2005). Secondly, they are made to complement each other in such a way that allows organizations to create an integrated management system. This means, a unique management system that complies with more than one of the rules or standards of management (Brewer & Nash, 2005). Thirdly, due to the compatibility among the rules, it becomes easy to companies with experience in implementing a management system, to do it with any of the others.

Fourthly, all management systems can be certified according to governing law and evidence of companies. Their implementation and certification hold a positive impact in their performance (Nicolau and Sellers, 2002). The essential premise of certification in ISO 9001/14001/2001 Rules is that the process of creation of products and services can be managed using any of the systems because their receipts and expenditures can be measured in several moments while the system adds value (Stevenson & Barnes, 2002). Fifthly, such rules are made to be applicable to any type of organization, that is to say, big, medium or small ones (Humphreys, 2005) and to any scope of business.

Particularly, and related to Information Security, these rules are respectively, the code of practice for the security management of information (ISO 17799) and the requirements of security of the Security Systems of Information (ISO 27001) and now the Guide ISO 31000 because it has been accepted that there is a very close link between information security and risk management and these rules help this relation (Saint-Germain, 2005).

3.2.1. ISO 27000 Standard

Due to the importance that information security has in organizations and with the purpose of facing malicious intruders that enter into them to do damage, best practices around setting security standards of information related to ISOIES BS7799-IT, RFC2196, Baseline, SSE-CMM and ISO 27001, the most relevant in IT information security has been identified (Diaz, 2008).

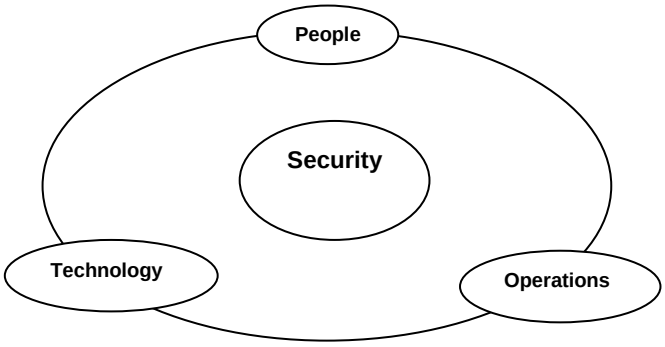
The purpose of information security is to protect resources of an organization such as hardware, software and people. By selecting and applying suitable security, organizations can reach their objectives or missions when they protect their physical and financial resources, reputation, legal position, employees and other tangible and intangible assets. The security systems of information start and end with the people within the organization and with the people who interact with the system (Shubhalaxmi, 2011). Thus, information security must be considered as a way of protecting assets of a business and at the same time a strategic element to add value to companies and keep them competitive in the market (Nicolau & Sellers, 2002)

Because of their economic activity and under the premise that emphasizes the importance of information within organizations, there is a need within organizations of designing mechanisms that allow to guarantee confidentiality, integrity and availability of information that it is handled and protect the assets of information by implementing suitable processes within a company.

On the whole, the elements that interact within the security of an organization are people, technology and operations or processes. That is to say the security of an organization is the result of operations made by people and supported by technology. The main reason of security of information is to protect the information assets by implementing suitable processes within the organization (ISO, 2005b)

[87] Mc Clean, Chris. *ISO 31000 – The New, Streamlined Risk Management Standard*.2010.

Graph 9. ELEMENTS OF SECURITY IN THE ORGANIZATION



Source: AENOR Perú.

ISO / IEC 27001 standard has been developed to protect information assets of organizations (Humphreys, 2005). A critical indicator of Information Security in companies is shown in empirical results: 50% of companies that lose their critical systems of business for over 10 days do not recover them at all and get out of business (Louderback, 2005). This announcement impacted the world of information security (Humphreys, 2005). ISO / IEC 27001, recently introduced (in 2005) is a revised version of the British rules BS 7799-2 published by British Standards Institution (BSI) in 1999. By this way, the rule targeted at Management of Information Security has the objective of helping state and maintain an information system of efficient management, using an approach of continuous improvement. In Annex A of the Rule, 11 domains, 39 control targets and 133 controls that an organization should bear in mind to implement an Information Security Management System, are defined (ISO, 2005a)

To implement an Information Security Management System (ISMS) according to ISO 27001 Rule is important that the organization has suitably defined the tools used to identify the actual risk and the methodology to measure that risk and that they should be held in time and do not obstacle labor in future. Methodology and tools must be made according to the criteria of the organization and related to the main activity or core business (Lizarzaburu E, 2011)

Long before ISO / IEC 27001 was published, it was already known that this type of rule was what companies were looking forward (Humphreys, 2005). In fact, it was designed to be practical and flexible enough to be assembled with the actual management systems and suitable to any approach of risk that the organization can adopt. (Humphreys, 2005)

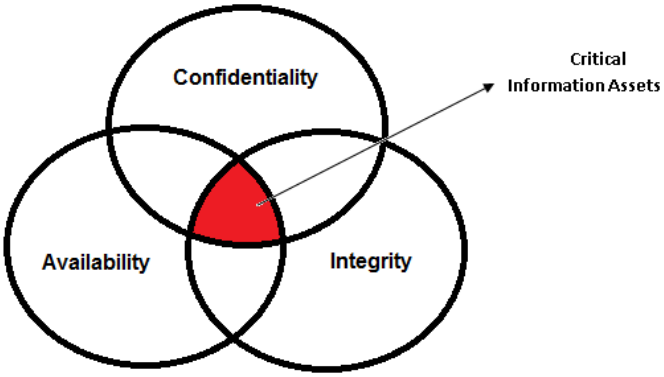
3.2.2. Information Security Management System

ISO 27001 Standard states the requirements of how an organization can implement the security requirements of ISO 17799:2005 Rule. According to ISO 27001 standard (Lineman, 2007) "This rule has been designed to provide with a model to state, implement, operate, supervise, revise, keep and improve an Information Security Management System (ISMS)". As per this Rule, Information Security Management is defined as: "The management system includes the organization structure, the policies, planning activities, responsibilities, practices, procedures and resources".

This rule can contribute to develop an approach of risk management based on the selection, implementation, revision and follow-up of strict controls. Development of ISMS and an "approach based on risk" are processes that require an important investment of time (Shubhalaxmi, 2011).

In other words, ISMS extends through all the program of information security, including their relation with other parts of the organization. Whereas ISO 27001 does not provide with a complete procedure for a security program of suitable information, but numbers each of the different organization functions necessary for certification, including a list of required documents that must be made, ISO 27001 uses an approach based on processes, duplicating the model defined for the first time by the organization for Cooperation and Economic Development (OCDE). The cycle Plan – Do – Check – Act (PDCA) (OCDE, 2002) divides the general processes of organization in four phases. A process that must be followed to ensure that ISMS, and by default, risk management must not be static processes (Shubhalaxmi, 2011).

Graph 10. ISMS: ISMS ESSENTIAL PRINCIPLES



Source: Calder, A. Information Security base on ISO27001/27002: A Management Guide.

MSIS adoption helps the company to develop measures to reduce the weaknesses related to the Information Security such as: physical access or information without restrictions, lack of information backup, incomplete activity records, lack of a clear separation of responsibilities and functions, among others. While more information is created, processed and stored digitally and a larger amount of income of the companies is promoted by critical processes of information, ISO / IEC 27001 rule becomes more important because it allows to identify and consider the risk to which information systems, assets or services of the companies are exposed, with the purpose of identifying and selecting suitable appropriate controls to protect information (De Freitas, 2009).

ISO / IED 27001 can be appreciated as a whole programme that combines risk management, security management, administration and accomplishment. It helps company to ensure that suitable people, process and systems are in their place, and to ease a proactive approach to manage the security and risk (Benner, 2007).

3.2.3. ISO 31000 Guide

In November 2009, the International Organization of Standardization published ISO 31000:2009 Guide (Risk Management – Principles and guidelines) that states a reference frame designed to explain the elements of a program of efficient risk management. The reference frames previous to ISO 31000:2009 include COSO methodology, ERM and AS / NZS 4360 Risk Management Standard. Unlike them, ISO Rule provides a simplified guide of reference about the principles and processes of management risk although it is not certifiable.

With the implementation of ISO 31000, the organization is able to clearly define the terms[88] related to Risk Management that are applicable in order to remove the obstacles in the fulfillment, audits and business duties; to review continually the processes that are related to the control of risk so as to identify improvement soon; to make the organization aware of the importance of risk management to all groups of interest of the organization; and finally, to identify and assess uncertain events that promote a positive impact within the organization; by this way, ISO 31000 Rule becomes a valuable management tool for the organization because it helps mitigate risk and increase the positive impact for the organization.(Lizarzaburu E, 2011)

That is to say, the rule will help professionals in the field of risks so as to define terminology clearly, to state formal processes, to understand the context of efforts and to consider the inherent opportunities in risk. Although this first version does not help to develop practical tools of risk management, their scope is complete in relation to the description of risk that can lead to the implementation of a program of risk management.

To sum up ISO 31000 allows:

- **To achieve an agreement about the definitions within a group of terms related to risk management**: this terminology is provided by the Guide ISO 73:2009 - Risk Management – Vocabulary[89] whose information will help to remove the idiomatic obstacles that exist among fulfillment, audits and business duties.
- **To review processes related to risk control**: It is likely that many of the processes described in ISO 31000 Rule are already part of the program of risk management but it is possible that the rule provides recommendations for their revision and identify opportunities of improvement.
- **To set practices of risk management in the appropriate context**: to understand the importance of risk management in the organization, their context must be identified in an internal and external background which implies strategy, then management, information systems and culture.

[88] ISO Guide 73:2009 Risk Management – Vocabulary (http://www.iso.org/iso/iso_catalogue).

[89] ISO Guide 73:2009 Risk Management – Vocabulary (http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=44651)

- **To consider risk as potentially positive or negative uncertainty (upward and downward risks):** This is specially complicated in areas of operative risk but processes and definitions that provide to ISO 31000 can be used to assess uncertain events or circumstances that may affect business objectives positively. The process of taking this into practice can take much longer but it is the best way that risk management becomes a valuable tool for decision making more than just mitigation of the loss or fraud.

However, the great obstacle that organizations face when implementing ISO 31000 consists of translating their concepts in tools, methodologies and processes that are appropriate for the organization for implementing the guide. Organizations must identify the most important risks. It is rather a complex duty for organizations if appropriate methodology has not been clearly defined and can be understood for future. It is important not to make their applicability difficult when identifying and assessing new possible scenarios that may affect the organization positively or negatively (Lizarzaburu E, 2011).

3.3. Project Management

Many researchers (Fox and Waldt, 2007; Schoen et al., 2005, Lytras and Pouloudi, 2003) have analyzed the development of planning techniques for Project management. One example is the Critical Path Method (CPM), the Project Evaluation and Revision Technique (PERT) created in 1950, and the introduction of Gantt chart of Henry Gantt in 1958.

On the whole, according to Soderlund (20039, the historic development in the Project Management (PM) implies that the Project Management is "a method of solving specific problems of delimitation or group of activities by the use of several types of techniques and methods" (Karapetyan & Otieno, 2011).

In 1976, the first organism of Project management was set up in the United States by PMBOK Guide of Project Management Institute (PMI). Since then, the PMBOK Guide has been a guide for practices of project management and emphasizes on time, cost and scope; and the use of focus of systems (Jugdev, 2004). Similar associations have been developed in several countries such as the International Project Association (IPMA), Association of Project Management (APM) among others.

Within schools Project Management suggested by Bredillet (2007, 2008), the evolution and influence of PM is shown in other management disciplines. Bredillet points out that there is a need to classify research trends in project management to current developments in PM as for example; knowledge bodies, certification programmes and educational programmes can act as a source of value creation for the organization. All the different views on project management represent heterogeneity and the need of application of different tools and techniques. Depending on the school meets the needs of the project best; it is chosen the appropriate PM approach.

Thus, the concept of project management changes over time and becomes a specialized form of management as well as other functional strategies. It is used to achieve business objectives within a defined budget program. The essence of project management is to support the implementation of the competitive strategy of an organization to provide a desired result (Milosevic, 2003). Compared to the traditional stereotype, the recent literature recognizes project management as a key business process (Jamieson & Morris, 2004).

This approach defines an organization as a process rather than a function or matrix and describes project management as one of the key business processes that enable companies to implement systems that increase value. Therefore, when organizations link their projects to business strategy, are better able to achieve their organizational goals (Srivannaboon, 2006).

The focus of the PMI Project Management identifies the elements of project management that organizations must match with their business strategy to manage risks appropriately. PMI defines a project as a temporary effort carried out to create a product, service or result.

Table 3. SUMMARY OF THE 9 SCHOOLS OF THOUGHT OF PROJECT MANAGEMENT

School	Metaphor	Central Idea	It became known	Key Analysis Unit (Bredillet, 2010)
Optimization	Project as machine	Analysis of the components of the project, planning and programming. (Anbari et al, 2008) Optimizing project results using mathematical methods (Bredillet, 2010).	At the end of the 40s	Time
Modeling	Project as mirror	Organizational factors, behavioral and political issues that affect projects. Use of systems for projects modeling. (Bredillet, 2008c).	Hardware Systems: In the middle of the 50's./Software Systems: In the middle of the 90's	Time, cost, performance, quality, risk, etc.
Government	Project as Legal Entity	Client-Employer relationships, transaction costs within the project management, program and portfolio (Anbari et al,. 2008).	Contracts: In the early 70's/ Management: In the middle of the 90's	The project, participants and management mechanisms.
Behavior	Project as a Social System	Leadership, communication, teamwork and human resource management, virtual team, multicultural issues.(Bredillet, 2008d).	Human Resources Management: In the early 2000	People and work teams
Success	Project as Business Objective	Success factors and criteria of projects, satisfaction of the interest groups and reasons for project failure (Bredillet, 2008d).	In the middle of the 80's	Success criteria and factors
Decision	As Computer Project	Information processing during the project life cycle, methods of estimation of cost and time realistic (Bredillet, 2008e).	At the end of the 80 decade	Information on which decisions are made
Process	As Algorithm Project	Find the right path towards fulfilling the vision; analyze them for the optimization of the main processes (Bredillet, 2008e).	At the end of the 80 decade	The project, its processes and threads
Contingencies	As Chameleon Project	Distinguish the types of projects to adapt management processes of appropriate projects; match capacities with strategy (Anbari, et al., 2008).	Early in the decade of 90	Factors that differentiate projects
Marketing	Project and Advertising	Analysis of the needs of individual interest groups, internal and external marketing projects (Anbari, et al., 2008).	Group of interest: In the middle of the 90's/ Board of Directors: In early 2000	Commitment of interest groups in projects and project management

Source: Karapetyan, A. y Otieno, R. (2011). A Study of Knowledge Management Challenges in Project Management: Case of Start-up Projects in Swedish Incubators, University essay from Umeå universitet

3.3.1. General Concepts[90]

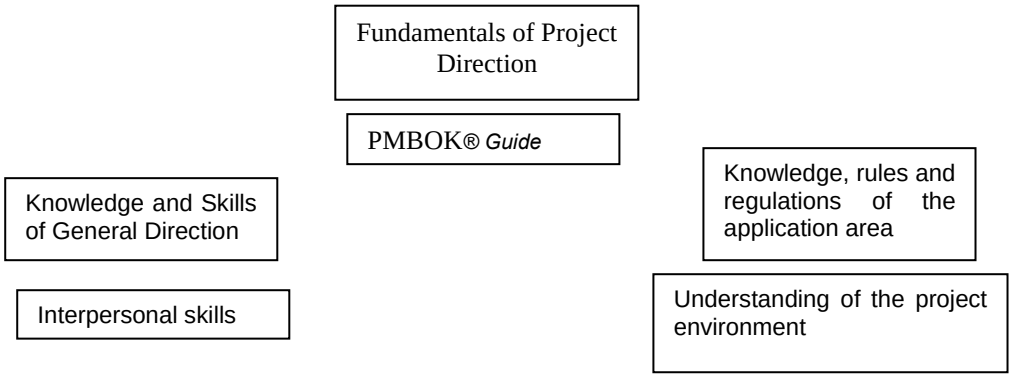
PMI defines a project as a temporary endeavor carried out to create a product, service or result.

From this definition it can release three essential concepts such as time, the results, the scope and impact.

The Project Risk Management Institute (PMI) suggests through the PMBOK identify the fundamentals of project management, recognized as the result of a summary of good practices.

[90] De los Ríos, M, Risk Management Plan for the construction of tunnel of upper conduction in hydroelectric Project el Diquís hydroelectric project of Instituto Costarricense de Electricidad, Universidad para la Cooperación Internacional. 2009.

Graph 11. PMI: FUNDAMENTALS OF PROJECT MANAGEMENT



Source: PMBOK®

The PMBOK ® says that these practices can be applied to most projects and there is consensus about their value and usefulness. However, each project will depend on the way to be implemented, that is why there must be a project management team trained to respond to each project in the best way.

The PMBOK ® divides project direction in 9 areas of knowledge[91] that by integrating management of the project are properly unified to create the Project Management Plan.

One of these areas of knowledge is the Managing Project Risk. Area that is analyzed in the current document. Risk Management consists of six processes: (i) Planning, (ii) Identification, (iii) Qualitative Analysis, (iv) Quantitative Analysis, (v) Planning of Response (vi) Monitoring and Control.

3.3.2. Project Risk Management

Project Risk Management according to PMI is the process of identifying and analyzing risks and response, monitoring and control them.

Among the key concepts[92] within the Project Risk Management should consider: the risk of project or any event or condition that can negatively impact the objectives of a project, the risk event or isolated event that can impact the project in a positive or negative and risk status or situation in which the risk is present.

Related to this, PMBOK defines and identifies six processes of Project Risk Management:

- **Planning and Risk Management**: State the project environment to define approach that will be used to evaluate, analyze the activities of risk management project.
- **Identification of Risks**: Identify risks that may affect the project and document their characteristics. The identification is done by selecting a tool for detection as: Interviews to experts, Checklists, Brainstorming, among others.
- **Risk Qualitative Analysis**: Prioritize risks identified for analysis according to the probability or frequency of occurrence and significance of their impact. From this point, a risk evaluation matrix must be developed obtained from the resulting probability –impact combinations
- **Risk Qualitative Analysis**: Objectively analyze the effect of identified risks according to information from the data collected.
- **Risk Response planning**: Develop strategies according to risk profile of the organization. That is, to choose alternatives to take advantage of opportunities and reduce threats that may be identified in the project.
- **Risk Monitoring and Control**: Tracking identified risks, monitoring residual risks according to the selected controls, identify new risks, execute plans to respond to the risks and evaluate their effectiveness throughout the project life cycle.

Three basic strategies for dealing with risks are defined whose effects could negatively impact the project objectives: avoid, transfer, and mitigate.

4. Discussion and Conclusions

At present and following the change from Basel II to Basel III, the use of standardized methods for handling and monitoring risks is being reviewed by different organizations from the ISO to PMI, which reflects its current importance.

Regarding the level of implementation of standards in different Latin American countries, it has not been reviewed in this research and is important in view of new regulations on the financial international crisis has caused in several regulators.

[91] Integration Management, Scope Management, Time Management, Cost Management, Quality Management, Human Resource Management, Communications Management, Risk Management and Procurement Management Project.

[92] Project & Process Management Consulting International, Risk Management for Project Manager, PMI, 2008.

While there is concern, from the revision of the degree of penetration of the rules and standards, it is still not high and the companies, especially in emerging countries, must rely on internal database instead of international standards.

The human factor is an important variable in setting internal policies design. Although in this paper we have appreciated a relation of current regulation, their impact on people who are going to implement and facilitators, has not been worked and could be a line of future research.

References

1. AENOR Perú. (2011). UNE ISO/IEC 27001:2007, Rule Interpretation AENOR Perú formación.
2. Alvarez, F. & García, P. (2007). Implementation of Information Security System based on ISO 27001 rule, for Intranet of Corporación Metropolitana de Salud. Escuela Politécnica Nacional.
3. Anbari, F. T., Bredillet, C. N. and Turner, J. R. (2008). Perspectives on Research in Project Management. Academy of Management Proceedings, 1-6.
4. Archer, N., & Ghasemzadeh, F. (1999). An integrated framework for project portfolio selection. International Journal of Project Management, 17(4), 207 – 216.
5. Beasley, M.S., Clune R. & Hermanson D.R., (2006). The impact of Enterprise Risk Management on the Internal Audit Function. Strategic Finance, 1-26.
6. Benner, J. (2007). ISO 27001: Risk management and compliance. Risk Management Magazine, 55, 24-29.
7. Bowling D. y Rieger, L. (2005). Making sense of COSO's New Framework for Enterprise Risk Management, Bank accounting & Finance.
8. Bredillet, C.N. (2007) Exploring research in project management: Nine schools of project management research (part 3). Project Management Journal, Dec2007; 38 (4), 2-4.
9. Bredillet, C.N. (2008d) Exploring research in project management: Nine schools of project management research (part 4). Project Management Journal; Mar2008, 39 (1), 2-6.
10. Bredillet, C.N. (2008e) Exploring research in project management: Nine schools of project management research (part 5). Project Management Journal; Jun2008, 39(2), 2-4.
11. Bredillet, C.N. (2010). Blowing Hot and Cold on Project Management. Project Management Journal; Jun2010, 41(3), 4-20.
12. Brewer, D., & Nash, M. (2005). The similarity between ISO 9001 and BS 7799-2: Gamma Secure Systems Ltd.
13. Calder, A. (2009). Information Security base on ISO27001/27002: A Management Guide, Van Harem Publishing.
14. Committee of Sponsoring Organizations of the Treadway Commission. (2004). Enterprise Risk Management Integrated Framework.
15. Cooper, D. (2005). Project Risk Management Guidelines – Managing Risk in Large Projects and Complex Procurements. John Wiley & Sons.
16. De Freitas, V. (2009). Analysis and information risk evaluation: study case: Universidad Simón Bolívar. Link: Revista Venezolana de Información, Tecnología y Conocimiento, 6 (1), 43-55.
17. De los Ríos, M. (2009). Risk Management Plan for the contruction of the tunnel of upper conduction in hydro-electrical Project el Diquís del Instituto Costarricense de Electricidad, Universidad para la Cooperación Internacional.
18. Díaz, F. (2008). Main Standards for Information Security IT: Essential scope and considerations of standards ISO-IEC BS7799-IT, RFC2196, IT BASELINE, SSE-CCM y, ISO 27001. Eos, 2(33), 77-109.
19. Díaz, J. (2005). Sarbanes-Oxley Law and audits. Partida Doble, 169(6), 104-109.
20. Ernst & Young, (2011). Training in Interno Coso Control.
21. Flaherty John J. (2004). Enterprise Risk Management – Integrated Framework: Executive Summary September.
22. Fomin V V, de Vries H, & Barlette Y. (2008). "ISO/IEC 27001 Information Systems Security Management Standard: Exploring the Reasons for Low Adoption", EUROMOT 2008 Conference, Nice, France.
23. Gupta, Parveen P., COSO 1992 Control Framework and Management Reporting on Internal Control: Survey and Analysis of Implementation Practices (June 10, 2009). Published as a Research Monograph by the Institute of Management Accountants in U.S.A. Available at SSRN: http://ssrn.com/abstract=1417604.
24. Humphreys, T. (2005). State-of-the-art information security management system with ISO/IEC 27001:2005. ISO Management Systems, 15-18.
25. ISO. (2005a). ISO/IEC 27001:2005. Information technology - security techniques - information security management systems - requirements. Geneva: International Organization for Standardization.
26. ISO. (2005b). The ISO survey - 2005. Geneve: ISO Central Secretariat.
27. Jacquelin Bisson and Rene Saint German, 'The BS7799/ ISO 17799 Standard for better approach to Information Security`, Pg.5, www.callio.com, posted on 15th June 2004, retrieved on 16th July 2006.
28. Jamieson, A., & Morris, P. W. G. (2004). Moving from corporate strategy to project strategy. In P. W. G. Morris and J. K. Pinto (Eds.), The Wiley guide to managing projects (177 – 205). Hoboken, NJ: John Wiley & Sons, Inc.
29. Jugdev, K. (2004). Through The Looking Glass: Examining Theory Development in Project Management with the Resource-Based View Lens. Project Management Journal, September 2004. 35(3), 15-26, ISSN 8756-9728/03.
30. Karapetyan, A. y Otieno, R. (2011). A Study of Knowledge Management Challenges in Project Management: Case of Start-up Projects in Swedish Incubators, University essay from Umeå universitet.
31. Knight, F.H. (1921) Risk, Uncertainty, and Profit. Boston, MA: Hart, Schaffner & Marx; Houghton Mifflin Company.
32. Laakso, P. (2010). ERM – form Risk Management to Leading the Opportunities. Laurea University of Applied Sciences.
33. Louderback, J. (1995). Will you be ready when disaster strikes? PC Week, 12, 130-131.

34. Liebenberg A.P. y Hoyt R.E. (2003). The determinants of enterprise risk management: Evidence from the appointment of chief risk officers. Risk Management and Insurance Review, 6(1), 37-52. Retrieved October 13, 2008, from ABI/INFORM Global database.
35. Lemieux, V. (2010). The record-risk nexus: exploring the relationship between records and risk,. Record Management Journal .20(2), 199-216.
36. Lineman, D. Information Security Policies Made It Easy [ISPME], for ISO 27001, Pg [1-2], Information Shield Publication, posted on 28th March 2006, www.informationshied.com, retrieved on 30th April 2007.
37. Lizarzaburu, Edmundo R., Quality Services Implementation: Peruvian Experience – OTC Market (August 8, 2011). Available at SSRN: http://ssrn.com/abstract=1906836.
38. Michaneal E.Whiteman and Herbert J. Maltord, Principles of Information Security, Second edition 2007, Thomson Technology, India Edition, Pg. [198-199].
39. Milosevic, D. Z. (2003). Project management toolbox: Tools and techniques for the practicing project manager. Hoboken, NJ: John Wiley & Sons.
40. Moeller, R. (2007). COSO Enterprise Risk Management: Understanding the new integrated ERM framework, John Wiley and Sons.
41. Nicolau, J. L., & Sellers, R. (2002). The stock market's reaction to quality certification: Empirical evidence from Spain. European Journal of Operational Research, 142(3), 632-641.
42. OECD Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002. [www.oecd.org].
43. Pagach, D. y Warr, R. (2007). An Empirical Investigation of the Characteristics of Firms Adopting Enterprise Risk Management. North Carolina State University Working paper.
44. Pagach, D. y Warr, R. (2008). The Effects of Enterprise Risk Management on Firm Performance.
45. PMBOK. (2004), Appendix A.
46. Porthin, M. (2004). Advanced Case Studies in Risk Management. Helsinki University of Technology: Department of Engineering Physics and Mathematics.
47. Roisenzvit, A. y Zárate, M. (2006). To a culture of Risk Management: Next challenge for the región and how it affects FSAP, ASBA evaluation processes.
48. Pessolani, P. (2007). Ris Evaluation in Information Technology and Communications aimed at Public Bodies. Speech presented in IV Congreso Iberoamericano de Seguridad de la Información. Mar del Plata. Argentina. 245-259.
49. Root, Steven. (1998). Beyond COSO: Internal Control to Enhance Corporate Governance. New York: John Wiley & Sons, p. ix.
50. Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. Information Management Journal, 39(4), 60-66.
51. Sema Group (2006). MAP-Magerit Version 2, Mehodology of Analysis and Risk Management of Information Systems - Secretaría del Consejo Superior de Administración Electrónica. Ministerio de Administraciones Públicas. Madrid. España.
52. Shubhalaxmi, J. (2011). A Study of information security policies in selected it companies in pune city, University of Pune.
53. Soderlund, J. (2004). Building theories of project management: past research, questions for the future. International Journal of Project Management, 22: 183–191.
54. Srivannaboon, S. (2006). Linking Project Management with Business Strategy, PMI Global Congress Proceedings.
55. Stevenson, T. H., & Barnes, F. C. (2002). What industrial marketers need to know now about ISO 9000 certification – a review, update, and integration with marketing. Industrial Marketing Management, 31(8), 695-703.
56. von Solms, B., & von Solms, R. (2005). From information security to... Business security. Computers & Security, 24, 271-273.
57. Wagner, Stephen, and Lee Dittmar. "The Unexpected Benefits of Sarbanes-Oxley." Harvard Business Review. April 2006, 133-140.
58. Walker, P.L., Shenkir, W.G., Barton, T.L. (2003). ERM in Practice. Internal Auditor; 60, 4; ABI/INFORM Global.
59. Wan Norhayate Wan Daud and Ahmad Shukri Yazid, (2009), "A Conceptual Framework for the Adoption of Enterprise Risk Management in Government-Linked Companies", International Review of Business Research Papers, Vol. 5, No. 5, September, 229 – 238.
60. Williamson, D. (2007). The COSO ERM Framework: A critique from systems theory of management control, International Journal of Risk Assessment and Management, 7(8).
61. Yates, JoAnne and Murphy, Craig N., Coordinating International Standards: The Formation of the ISO (January 2007). MIT Sloan Research Paper No. 4638-07.