A Conceptual Model to Manage Insurers' Operational Risk

Dr. Mahmoud Asad Samani[1]

Abstract

The insurance business has to be done in a prudent manner and under supervision by a regulatory body so that a minimum solvency and the business continuity requirements are maintained. The European Solvency II requirements need an insurer to have in place an effective risk management system. Credit, market, insurance and operational risks are the main categories of risks which an insurance business is facing. In this paper, the Solvency II requirements for risk management, definition of operational risk and the Risk Management Standard ISO 31000:2009 as a useful guideline for managing operational risks are discussed. Operational risk is enterprise-wide risk. It can include classes of risk, such as fraud, security, privacy protection, legal risks, physical (e.g. infrastructure shutdown) or environmental risks. It is shown that ISO 31000 can effectively be applied to manage the insurer's operational risks. A conceptual model for operational risk management is introduced and the model is tested by a case study.

Keywords: Solvency II, Operational Risk Management (ORM), Risk-Based Capital (RBC), Own Risk and Solvency Assessment (ORSA), Risk Management System (RMS)

1. PhD in Industrial Engineering, Director General, Department of Risk Management Development, Central Insurance of I.R.Iran. samani002@gmail.com

I. Introduction

The fast growing technological advancement mostly in IT, intense global competition, ongoing changes in local, national and international legal frameworks, etc. have severely altered the organizational business environment. These all have created new risks for organizations that need immediate attention by all organizational levels. Also, they have transformed the way how managers perceive risks, because organizations that achieve success in this uncertain environment are those which give more attention to innovation, risk taking and entrepreneurship, and strive to develop a culture of change acceptance and adaptation in order to keep improving.

Insurance companies are facing the same risky situation. They also need to effectively react to environmental parameters. The insurer's main role is to positively contribute to the country economical well-being by accepting, sharing and managing risks which are normally underwritten for individuals and business entities. The insurance business has to be done in a prudent manner and under supervision by a regulatory body so that a minimum solvency and the business continuity requirements are maintained.

The new insurance regulation in Europe, Solvency II, has been developed as a harmonized prudential framework for insurance firms. It was introduced in 2009 to replace a patchwork of rules in the areas of life insurance, non-life insurance and reinsurance. Solvency II rules introduce prudential requirements tailored to the specific risks which each insurer bears. They promote transparency, comparability and competitiveness in the insurance sector. The framework consists of a directive, implementing rules and technical standards. The Solvency II is related to capital requirements, risk management and supervisory rules.

The Risk-Based Capital (RBC) requirements call for insurance companies to hold capital in relation to their risk profiles to guarantee that they have enough financial resources to withstand financial difficulties. The Governance and Risk Management requirements oblige companies to put in place an adequate and transparent governance system and to conduct their Own Risk and Solvency Assessment (ORSA) on a regular basis. Also Solvency II enables supervisors to review and evaluate whether insurance companies comply with the rules and requires these companies to report to supervisory authorities and disclose information publicly.

Solvency II is not just about capital. It is a comprehensive program of regulatory requirements for insurers, covering authorization, corporate governance, supervisory reporting, public disclosure and risk assessment and management, as well as solvency and reserving.

The Solvency II program is divided into three areas, known as pillars:

Table 1- Pillars of the European Solvency II

Pillar 1	Pillar 2	Pillar 3
Financial Requirements	**Governance & Supervision**	**Reporting & Disclosure**
• Two thresholds: - Solvency Capital Requirement (SCR) - Minimum Capital Requirement (MCR) • SCR is calculated using either a standard formula or, with regulatory approval, an internal model. • MCR is calculated as a linear function of specified variables: it cannot fall below 25%, or exceed 45% of an insurer's SCR. • There are also harmonized standards for the valuation of assets and liabilities.	• **Effective risk management system.** • Own Risk & Solvency Assessment (ORSA) • Supervisory review & intervention.	• Insurers required publishing details of the risks facing them, capital adequacy and risk management. • Transparency and open information are intended to assist market forces in imposing greater discipline on the industry.

Pillar 2 requires insurers to have an effective RM system as an important element of the strategy of sound corporate governance. The importance of RM is now even more obvious than any time before. For insurance companies, RM is more significant as they are facing diverse ranges of risks. If the insurance risk profile is left unattended, it might lead to serious difficulties in insurer's activities and processes and fail them to achieve their expected results. That is why in particular, boards of directors have begun to consider and evaluate the insurers' risk profiles in a regular basis.

Solvency II divides the main risk categories of an insurance company into four classes, i.e. credit, market, insurance and operational risks. This paper is about Operational Risk Management (ORM) in an insurance context. The first 3 classes of risk are not dealt with as the main focus of this paper is the ORM. Operational risk is characterized as those risks of losses which are arising from *inadequate or failed internal processes, people and systems*. More details on operational risks are given in below and it is shown that the RM Standard ISO 31000:2009 can effectively be used for the purpose of ORM.

Therefore, the ISO 31000 is discussed along the below lines following by a more detailed discussion on ORM. Then a conceptual model is introduced to show how ORM can be done in real practice. The model is tested by a case study selected from the insurance industry.

II. Literature Review

Within an organization, risk can be originated from different sources i.e. security problems, natural catastrophes, human errors, third-parties interferences, fluctuations in business environments, financial crises and turmoil, project risks, etc. (Alhawari et al., 2012). The current business environment is characterized by the element of change. The companies, including insurers, not only need to recognize the ongoing changes but also must change themselves and manage the associated risks as well. The organization's environment keeps changing frequently. The change and risk are closely interrelated. Change happens in all organizations regardless that they are large or small or what activities they do. Therefore, the change should be monitored in a constant basis. That monitoring should be focusing on identification, assessment and management of the respective risks threatening the interested parties and their changing needs and expectations also shall constantly be monitored (ISO 9004, 2009).

In line with ISO Guide 73:2009, the document providing risk-related terminologies and vocabularies, risk is defined as *effect of uncertainty on objectives* (ISO Guide 73, 2009). In this context, risk is an uncertain event or circumstance which might happen with some probability, and if occurs, leads to a positive or a negative consequence and at least affects one or more organizational objectives. Another but yet good example of risks are in projects. Elements of time, cost, quality, etc. are important and the project principal usually requires the relevant objectives of these parameters to be maintained (Project Management Institute, 2013). Along the lines of the above definition, any deviation from such objectives is also regarded as risk.
It is worthy to be emphasized that many definitions of risk and risk management are available. However, ISO Guide 73:2009 provides basic vocabulary to develop common understanding on RM concepts and terms among organizations and functions, and across different applications and types. The risk definition given in ISO Guide 73:2009 has 5 complementary notes as follows:
NOTE 1: An effect is a deviation from the expected - positive and/or negative.
NOTE 2: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).
NOTE 3: Risk is often characterized by reference to potential events and consequences or a combination of these.
NOTE 4: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.
NOTE 5: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

1. Risk and Objective

This definition links risks to objectives and can be applied when the objectives of the organization are comprehensive and fully stated. The objectives themselves need to be challenged and the assumptions on which they are based should be tested, as part of the RM process. Risks can impact an organization in the short, medium and long term. These risks are related to operations, tactics and strategy, respectively. Strategy sets out the long-term aims of the organization, and the strategic planning horizon for an organization will typically be 3, 5 or more years. Tactics define how an organization intends to achieve change. Therefore, tactical risks are typically associated with projects, mergers, acquisitions and product developments. Operations are the routine activities of the organization (AIRMIC, ALARM, ARM, 2010).
A risk might occur due to one or more causes that each cause can lead to various consequences. The circumstances under which an organization operates or a project is being run may contribute to a higher degree of risk. Alhawari et al. (2012) quoted the inefficient management disciplines, unsuitable and non-consistent MSs, concurrent conduction of several activities, abnormal dependencies on external resources and other uncontrollable elements are all example of those circumstances. Additionally, risk also relates to those events or occurrences that barrier the organization from materializing their objectives, goals and ambitions. Poor quality of product/service might acutely contribute to non-achievement of organizational objectives.
Risk and uncertainty are two sides of the same coin. The organizational lifecycle has been surrounded by risk. Risk exists in all the times and places within an organization. It is like a shadow chases a business. Therefore, it is too wise to identify the sources of risk, evaluate its frequency of occurrence and consequences.
Researchers commonly agree that risk has some features or attributes. Risk is analyzed by determining consequences and their likelihood, and other attributes of the risk (ISO 31000, 2009). Frequency or probability is one of the risk attributes or as it is called in some glossaries likelihood. Both probability of occurrence or frequency of occurrence is used. Severity or impact of the risk is another attribute which is also called consequence (Carbone and Tippett, 2004). Standard document ISO 31000:2009 recognizes two sides for risk, i.e. negative and positive sides. Olsson (2008) highlighted more details of these two dimensions. The risk is the product of

the outcome probability and its severity (Ni et al., 2003). In Project Management Body Of Knowledge (PMBOK), a project risk is defined as *an outcome or uncertain condition that once happens, causes positive or negative consequences on at least one aspect of the project, such as cost, scope, quality, etc.* (Segismundo and Miguel, 2008; Project Management Institute, 2013). Argued by other researchers, risk largely seems as organization /project obstacles and threats. For instance, risk also has been defined as an obstacle to success (Miles and Wilson Jr, 1998).

As there are risk surrounding all the human life and organizational activities, it is prudent and wise to think about its management. The RM evolvement has been so quick over the recent decades together with integration with the project management (Del Cano and de la Cruz, 2002). RM consists of planning, identification, analysis, responses, and monitoring and control on a project. RM by itself is an exclusive discipline, as it puts together understanding from a range of other businesses. This discipline utilizes a range of various methodologies for a particular case. RM is regarded as too important and the integral part of any business and highly recognized by the project management institutions (Del Cano and de la Cruz, 2002). Bruckner et al. (2001) supposed that RM is about strategies, methods and supporting tools enabling organizations to identify and control their risks to an acceptable level.

2. Risk Management Standard ISO 31000:2009

ISO 31000 does not intend to prescribe a new MS. Its intention is to integrate RM into overall organization MS. The main objective of RM is to recognize all possible risks within a project, business or associated with a product. RM involves grading the risks according to their significance, impact or seriousness, probability of occurrence and then arranges for the required actions to treat and control them.

Every individual aspect of a risk possibly can be documented in details for further actions (Cule et al., 2000). It is clear that no one can anticipate the occurrence of losses. Therefore, RM objective is to make sure that the possibility of risk occurrence during the execution of a project or conduction of the organization business is rare and hence to reduce losses to a satisfactory level. Any loss occurrence reflects that the RM objective has not been achieved which in turn prevent organization to achieve its ultimate goals. RM must effectively enable to manage and control all possible occurrences. Additionally, to be effective it is necessary that RM to be considered as the integral part of the management framework. One more point is the way by which risk events are being treated, valued, compared and mixed together. RM is aimed at to establish a comprehensive analysis to recognize the organization and project scope and identify a complete set of risk factors and make sure that they are properly organized to convey all the stakeholders and different risk perspectives.

Standard document ISO 31000 encompasses the requirement for a RMS. This standard demonstrates how to develop and implement a RMS in an organization. This Standard recommends that organizations should have a framework that integrates the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture (ISO 31000, 2009).

ISO Standard 31000 states that when RM is implemented and maintained with this standard it enables organizations to gain the following benefits:

i. the likelihood of achieving objectives is increased;
ii. proactive management is encouraged;
iii. the awareness level in regard to the need to identify and treat risk throughout the organization is enhanced;
iv. identification of opportunities and threats is improved;
v. a compatible platform to compare risk management practices between organizations and nations is achieved;
vi. legal and regulatory requirements in local and international basis is complied with;
vii. financial reporting is improved;
viii. governance is enhanced;

ix. stakeholder confidence and trust is improved;
x. a reliable basis for decision making and planning is achieved;
xi. controls are improved;
xii. allocation of resources for risk treatment will be more effective;
xiii. operational effectiveness and efficiency is improved;
xiv. OHS performance and environmental protection are enhanced;
xv. loss prevention and incident management are enhanced;
xvi. losses are minimized;
xvii. organizational learning is improved; and
xviii. organizational resilience is improved.

3. Principles, Framework and Processes in Risk Management Standard

3.1. Risk Management Principles

There are a lot of opinions in regard to RM and what does it involve, how RM can be implemented and what results it can achieve. The ISO Standard 31000:2009 has been developed to address all those questions (AIRMIC, ALARM, ARM, 2010). ISO 31000:2009 encompasses and provides components of a RMS. The ISO 31000 is based on a number of principles as follows:

xix. Create value;
xx. Integral part of organizational processes;
xxi. Part of decision making;
xxii. Explicitly addresses uncertainty;
xxiii. Systematic, structured and timely;
xxiv. Based on the best available information;
xxv. Tailored;
xxvi. Takes human and cultural factors into account;
xxvii. Transparent and inclusive;
xxviii. Dynamic, iterative and responsive to change; and
xxix. Facilitates continual improvement and enhancement of the organization.

As per second (ii) principle, RM is an essential or integral part of all processes in an organization. RM is not separate or stand-alone MS and is an integral part of the main activities and processes of an organization. RM is a significant part of management responsibility and vital to all organizational processes from top to bottom i.e. from strategic planning to all project and the change management processes.

Fig.1 shows the RM framework. ISO 31000 includes the required activities in RM implementation and continuous support of the RM process. The RM steps in ISO 31000 are initiated from mandate and commitment (clause 4.2) which is the Board responsibility and is followed by:

a. Design of framework for managing risk (Plan) (clause 4.3);
b. Implement RM (Do) (clause 4.4);
c. Monitoring and review of the framework (Check) (clause 4.5); and
d. Continual improvement of the framework (Act) (clause 4.6).

The RM steps are the same famous PDCA methodology or framework which is the life cycle for continuous improvement. RM framework which is suggested by ISO 31000 is based on PDCA which is similar to QMS framework in ISO 9001:2015. RM framework is not intended to recommend a separate and independent MS. The ISO 31000 intention is to help organization to integrate RM into its overall MS (ISO 31000, 2009).

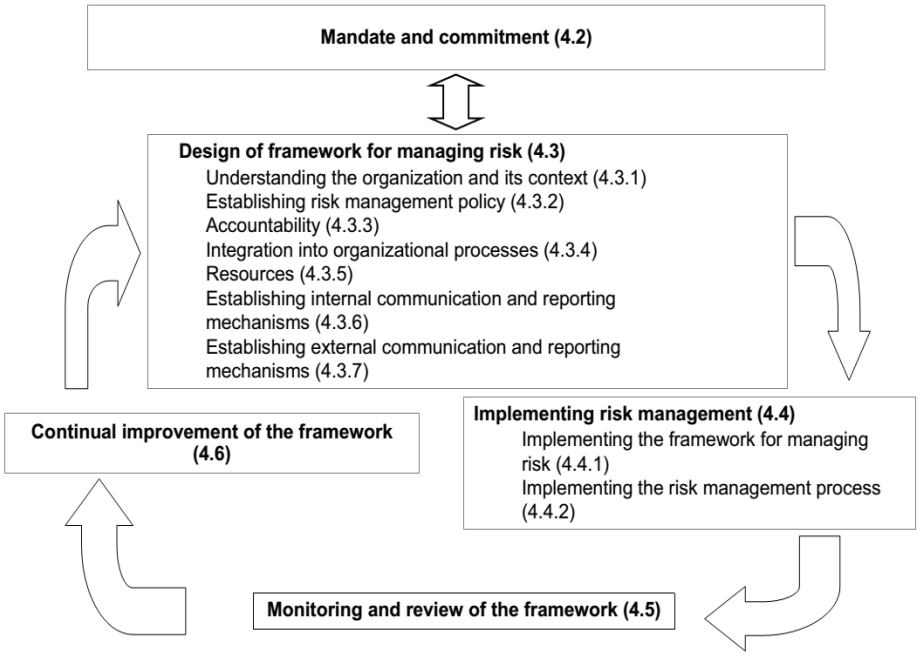

Figure 1. PDCA framework in RM standard (ISO 31000, 2009)

Clause 4.3.4 in ISO 31000:2009 requires RM to be embedded in all organization's practices and processes in a way that it is relevant, effective and efficient. The RM steps should become part of, and not separate from, those organizational processes. In particular, RM should be embedded into the policy development, business and strategic planning and review, and change management processes (ISO 31000, 2009).

3.2. Risk Management Process

Fig.2 shows the RM process suggested by ISO 31000 and its relevant clauses. ISO 31000 provides a framework for RM implementation not a framework to support the RM process (AIRMIC, ALARM, ARM, 2010). Looking into Fig.2 reveals the fact that RM process is nothing more than a PDCA framework. Clauses 5.2 and 5.3 can be looked upon as the *Planning* stage of PDCA. Clause 5.4 and its sub-clauses 5.4.2, 5.4.3 and 5.4.4 and the clause 5.5 comprise the *Do* stage and clause 5.6 encompasses the *Check* and *Act* stages of the PDCA methodology. The RM process in ISO 31000 doesn't determine how does RM process like, but rather it supports a framework for RM implementation. In fact, ISO 31000 suggest a PDCA framework to organizations to integrate the processes for RM into organizations' overall governance, strategy and planning, management, reporting processes, policies, values and culture (ISO 31000, 2009). In short, ISO 31000 is like ISO 14000 for EMS and OHSAS 18000 for OHSMS which are standards based on similar PDCA framework.

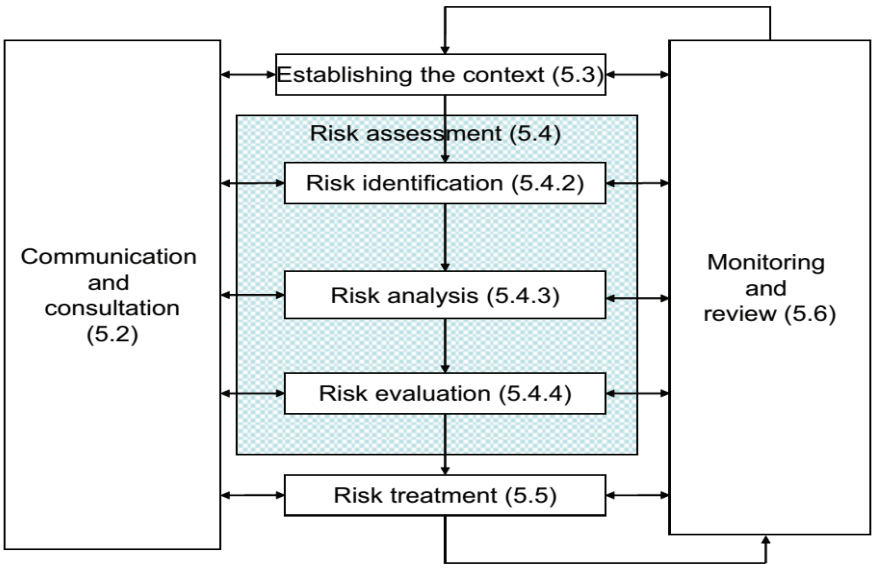

Figure 2. Risk Management process (ISO 31000, 2009)

Fig.3 depicts the same RM process with some more details and briefly shows what the contents of each step in RM process are. This figure has been reproduced from a document known as HB 436:2004 which is a companion text to previous RM standard AS/NZS 4360:2004 which was jointly developed by Australian and New Zealand Standard Organizations.

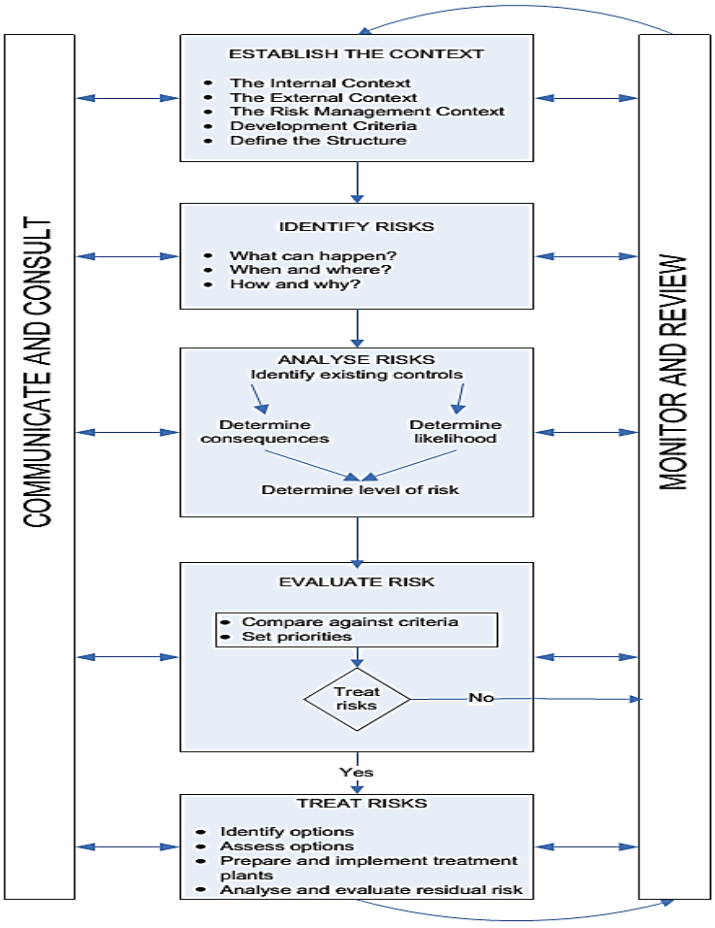

Figure 3. Risk management process in more detail (HB 436:2004)

To successfully implement RM framework in an organization, a number of parameters need to be taken into consideration. Fig.4 suggests the RM process shall consist of three important elements: *risk architecture* (means roles, responsibilities, communication and reporting structure, etc.), *risk strategy*

(i.e. appetite for risk, attitude, philosophy, etc. which must be defined and stipulated in RM policy) and *risk protocols* (means risk guidelines, rules and procedures, tools and techniques, etc.).

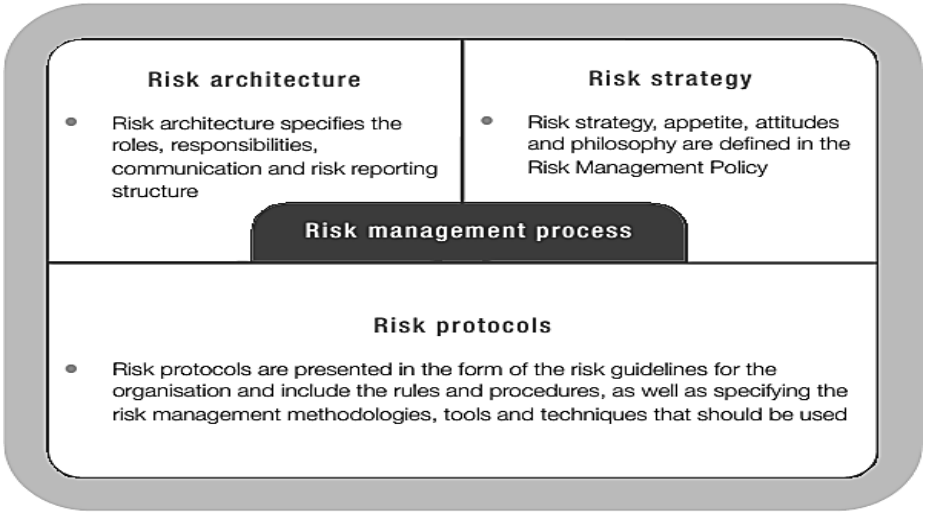

Figure 4. Risk architecture, strategy and protocols (AIRMIC, ALARM, ARM, 2010)

Fig.5 shows the principles, framework and the process model in RM Standard ISO 31000:2009. This figure suggests, RMS framework is on the basis of PDCA cycle and it employs a process model.

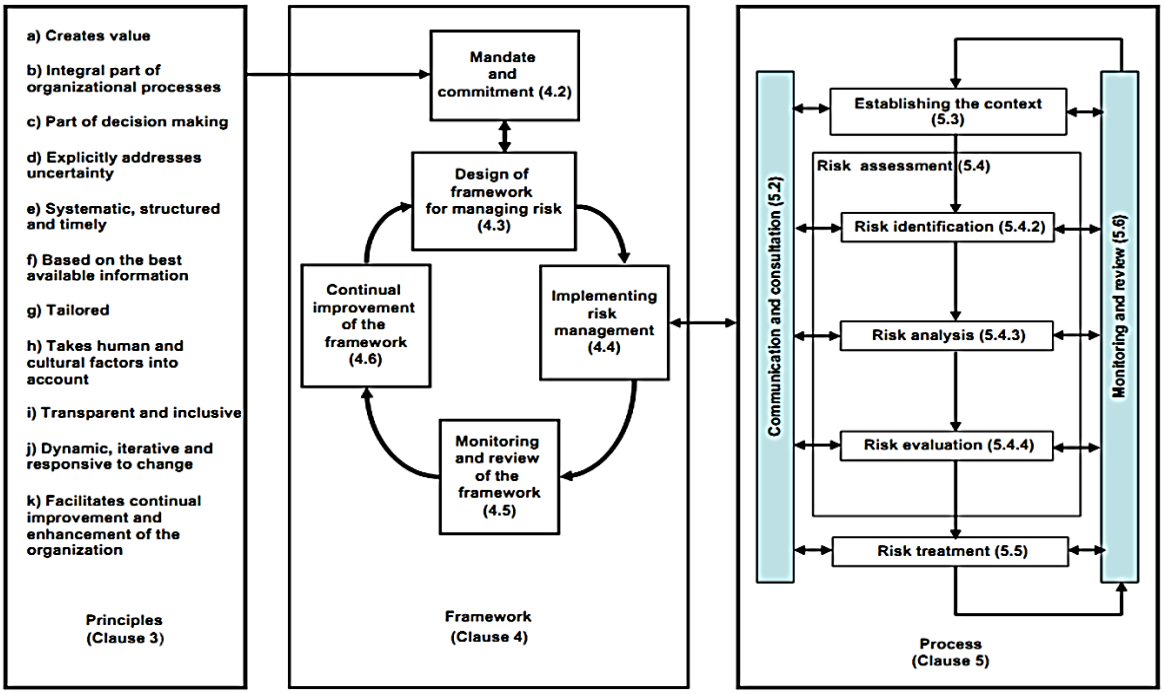

Figure 5. Relationship between RM principles, framework and process (ISO 31000, 2009)

RM is about strategies, methods and supporting tools to identify and control risk to an acceptable level. The main objective of RM is to recognize all possible risks within a project, business or associated with a process. To be effective, it is necessary that RM to be considered as the integral part of management framework.

4. Other Risk Management Standards

ISO 31000 is not the only RM standard. In 2004, an Enterprise Risk Management (ERM) standard was published by the Committee of Sponsoring Organizations of the Tread way Commission (COSO). RM practitioners are well known to the COSO ERM cube which provides

an ERM framework. The COSO ERM has been considerably influential as it has interlinks with the Sarbanes-Oxley Act requirements related to the companies listed in the US stock market (AIRMIC, ALARM, ARM, 2010). Other standard developers such CSA of Canada, JSA of Japan, AS/NZS of Australia and New Zealand, BSI of Britain, etc. have also developed RM standards.

5. Operational Risk Definition

In the Basel II regulations for banking system, operational risk is defined as *the risk of a change in value caused by the fact that actual losses, incurred for inadequate or failed internal processes, people and systems, or from external events (including legal risk), differ from the expected losses*. This definition, adopted by the European Union Solvency II Directive for insurers with some variation. Operational risk is enterprise-wide risk. It can include classes of risk, such as fraud, security, privacy protection, legal risks, physical (e.g. infrastructure shutdown) or environmental risks. Operational risk is a broad discipline, close to good management and quality management. In similar fashion, operational risks affect client satisfaction, reputation and shareholder value, all while increasing business volatility.

Contrary to other classes of insurance company risks (e.g. credit risk, market risk and insurance risk) operational risks are usually not willingly incurred nor are they revenue driven. Moreover, they are not diversifiable and cannot be laid off, meaning that, as long as people, systems and processes remain imperfect, operational risk cannot be fully eliminated.

Operational risk is, nonetheless, manageable as to keep losses within some level of risk tolerance (i.e. the amount of risk one is prepared to accept in pursuit of his objectives), determined by balancing the costs of improvement against the expected benefits.

Wider trends such as globalization, the expansion of the internet and the rise of social media, as well as the increasing demands for greater corporate accountability worldwide, reinforce the need for proper operational risk management.

III. Research Methodology

The intention of ISO 31000 is not to produce a separate MS but the aim is to integrate RMS into overall organizational processes (ISO 31000, 2009). This means RMS must be integrated into current organizational processes, i.e. in business development, pricing, customer relations, underwriting, claims handling, etc. RM involves grading the risks according to their significance, impact or seriousness, probability of occurrence and then arranges for the required actions to treat and control them.

The main objective of doing this paper is to find a reasonable and yet feasible answer to this essential question that how RM processes including identification, analysis, evaluation, control, etc. can effectively be integrated into the main stream organizational processes? For instance, how RM processes can be integrated into an insurance company underwriting processes? Definitely, the underwriting process encompasses a number of uncertainties which undermine the organization overall objectives. Inappropriate IT systems, incompetent human capitals, vague and ambiguous procedures and disciplines are just some uncertainty sources to name in a typical underwriting process. In one hand, ISO 31000 identifies these uncertainties as the sources of risks as they may potentially cause deviation in objectives achievement. In the other hand, these are ORs as originated from processes, people and systems. ORs affect client satisfaction, reputation and shareholder value, all while increasing business volatility.

The latest published ISO MSS RMS, i.e. ISO31000:2009, is generic and applicable to all organizations regardless of their size, type or product(s). RMS is based on PDCA architecture and the process approach. Derived from what so far has been stated, a conceptual model for ORM is given below and it is tested by a case study. The model is generic i.e. independent of the size, type, product, age and maturity of the organization in which it is going to be implemented.

IV. Results and Discussion

Fig. 6 below introduces a conceptual model for ORM. In essence, having established the RM context in an organization together with proper RM communication and consultation which are the ISO 31000 requirements, the risk assessment steps including risk identification, risk analysis and risk evaluation can be applied to every single processes. Doing so, will result in a risk registration and assessment tables like what was proposed in tables B and C in appendix. To identify the risks in a more formal and yet comprehensive manner, the guidelines like what was given in table A in appendix can also be applied. Next step is to set up risk treatment and action plans which can be developed like the format suggested in table D and tables E and F for reporting purposes (appendix).

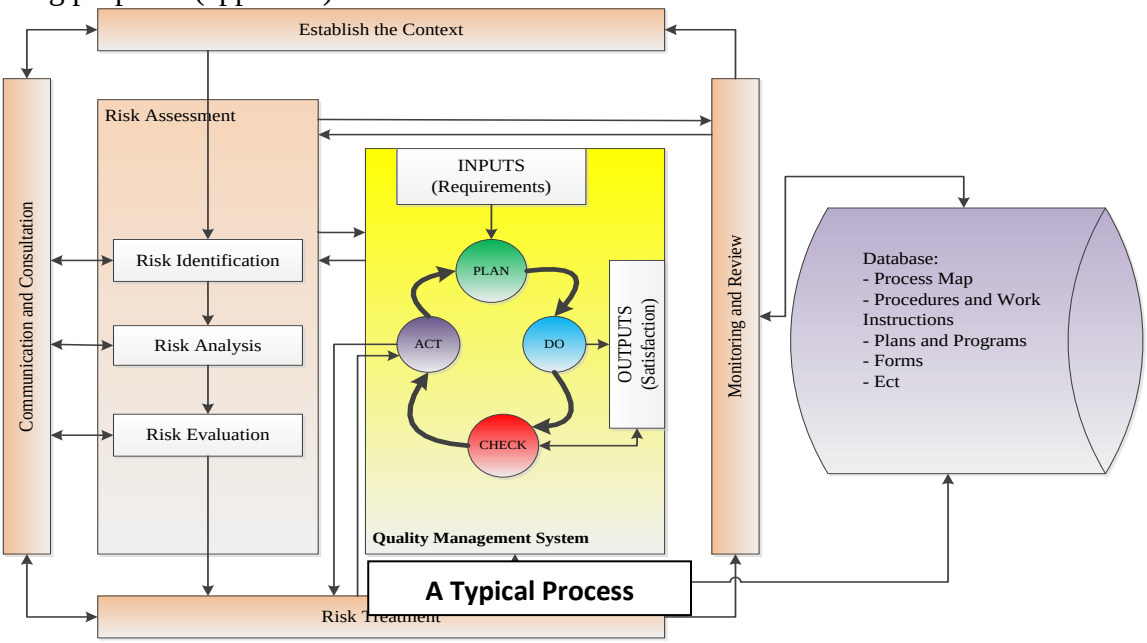

Figure 6. Risk Management Conceptual Model

1. Case Study: Application of the ORM Model on Strategic Planning for an Insurance Company

XYZ Insurance Co. was established in 2003. As an insurance company, XYZ philosophy is to provide the insurance services to the society, encourage competition in insurance industry, improve the insurance services to customers and boosting up the market insurance culture. The company is a direct insurer and has set up the reinsurance back-up as one of the key RM measures to safeguard the company financial integrity. Reinsurers protect direct insurers from disastrous losses and equip them up with higher insurance underwriting capacities. In this sense, XYZ has acquired reinsurance coverage from international leading and reputable reinsurers such as AON and Hannover-Re. The company mission is to provide all insurance services with emphasis on micro-insurances to the local and international markets with the optimum usage of the financial resources to generate more profits for company stakeholders. Their vision is to be the leading insurer with modern insurance products, positioned among the top 5 insurers in the country by 2025. The company objectives are listed as follows:

a) Promotion the insurance culture among all society levels;
b) Safeguard the national wealth and supporting the industrial and other entrepreneurs and caring about various investments by providing suitable insurance coverage;
c) Introducing new insurance coverage which are currently available in advanced industrial countries;
d) Up keeping the customer orientation principle by means of processes' automation and mechanization; and
e) Enhancement of the insurance penetration rate.

A typical strategic planning process is usually consisted of a number of fundamental phases which are presented as a sequence of rational series of phases with related activities in each phase. Fig. 7 suggests which phases can be typically taken into consideration when a strategic plan is going to be envisaged. The phases shown in Fig. 7 are not the only recipe to cook up a strategic plan. Different sources might suggest diverse activities or variants on these phases. However, the strategic planning process in Fig. 7 is general in nature and outlines the essential ingredients to build up a strategic plan and can be used by any organization regardless of their type, size or product.

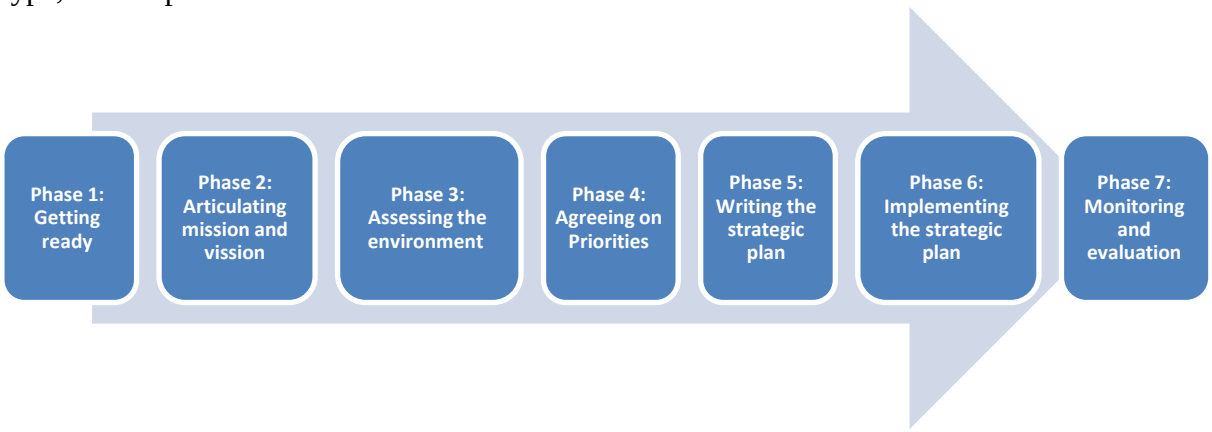

Figure 7. Typical phases in setting up a strategic plan

This process has 7 phases and 28 activities which for simplicity only 4 phases and 19 activities have been shown in table 2. Definitely, these activities and decision making points are the sources from which the risks might originate. Thus, the uncertainties associated with each activity or decision making and their likely consequences shall be identified to enable for taking other RM steps.

Table 2. Risk identification, likely consequences and suggested RM action plans for Horizon Company's strategic plan setting up process

Phase No.	Phase Name	Activities	Risk Sources	Likely Consequences
1	Getting ready	Identify reasons for planning Check readiness to plan Choose planning participants Summarize organization history and profile Identify information needed for strategic planning Write a "plan for planning"		
2	Articulating vision and mission	Write (or revisit) your mission statement Draft a vision statement		
3	Assessing the environment	Update information needed for planning Articulate previous and current strategies Gather input from external stakeholders Gather information about program effectiveness Identify additional strategic issues or questions		
4	Agreeing on priorities	Analyze interplay of strength, weaknesses, opportunities, and threats Analyze competitive strengths of programs Choose criteria for use in setting priorities Summarize the scope and scale of programs Write goals and objectives Develop long-range financial projections		

XYZ organizational strategies in macro level are: market penetration, market development and product development. The company strategies in operational (micro) level include the followings:

a. Marketing and sales (product, price, market and accessibility and incentives and promotions);
b. Financial services (financial support, investment, financing);
c. Distribution channels (recruitment, development);
d. Branding;
e. Society;
f. Human capital development (engagement, development and upkeep, rewarding);
g. Buildings and equipment;
h. Suppliers; and
i. IT

The company's macro and micro strategies as mentioned above have been developed as per table 3. The proposed ORM model has been applied to this process of strategy setting to further enhance the company's strategies in all organizational levels.

Table 3 - Strategies developed by XYZ Insurance Company

Strategies Main Category	Strategies Sub-category	Strategy Number	Strategy	Considerations
Marketing and sales	Product	S1	Portfolio development in all classes of insurance business	
		S2	Focus on specific classes of insurance	Life, fire, marine, liability, engineering, health, etc.
		S3	Propagation of internet based sales with focus on policies renewal	
		S4	Development of TPL and health insurances with loss ratio control	Non admittance of health insurances with poor records Loss ratio control for vehicles with poor loss records
		S5	Developing products to target specific groups	For specific clients For clients groups Packages for micro clients
		S6	High pricing for specific products	Tailored products New products
	Price	S7	Price discount and instalment for public classes with due notice to underwriting considerations	Regional pricing
		S8	Agencies development as per population distribution in country	
		S9	Increase in number of branches	
		S10	Risk and claim survey outsourcing in all classes	
	Market and accessibility	S11	Focus on specific markets in each class of business	Middle and high class people to be targeted for individual health and dentistry insurances Low loss ratio regions for fire insurance development Future banking market Motor bikes market Vehicles importers market Shipping and airlines Oil and gas companies and civil and industrial contractors for energy and engineering insurances

Strategies Main Category	Strategies Sub-category	Strategy Number	Strategy	Considerations
				Car manufacturers
		S12	FOC personal accident and fire household policies with life insurances	
	Incentives and promotions	S13	Profits sharing in relevant classes	
		S14	Pro-rata TPL policy	
		S15	Discount voucher for life insurance purchasers	
		S16	Festive ceremonies discounts	
		S17	Insureds club establishment and discount	
	Financial support	S18	Integrated payment system design and implementation	
		S19	Financial statements system design and implementation	
		S20	Warehousing system design and implementation	
Financial services		S21	Investment in construction projects	
	Investment	S22	Investment in securities market	
		S23	Savings in investment fund	
		S24	Investment in bank	
	Financing	S25	Capital increase by shareholders	
		S26	Increase in corporate agents	
	Absorb	S27	Increase in life promoter managers	
Distribution channels		S28	More effective interactions with brokers	
		S29	Balanced distribution of agents in provinces	
	Development	S30	Agents performance monitoring and rating	
		S31	Public and specific training to agents	
		S32	Enhanced presence in virtual space	
		S33	Advertisement in different media	
		S34	Informative and commercial flyers and brochures	
Branding		S35	Company web site improvement together with branches and agents web sites	
		S36	Attendance in national fairs like book fair	
		S37	Constant customer feedback evaluation	
Society		S39	Participating in insurance culture grooming (in line with regulator, insurance books publishing, focus on kids)	
		S40	Engagement and retaining talented people	
	Engagement	S41	Outsourcing some services, e.g. administration	
		S42	Balancing the organizational structure with the activities volume	
Human capitals		S43	Periodical training to enrich human capitals	
	Development and upkeep	S44	Promotion encouragement	
		S45	Welfare facilities enhancement (scholarship, long-term loans, discounts in insurance policies)	
	Rewarding	S46	Wage payment system restructuring	
Buildings and equipment		S47	Assimilation of buildings and equipment in branches (shape, color, appearance)	
		S48	Owning of buildings (purchase, build up)	
Suppliers		S49	Identification of appropriate suppliers for risk and claim survey	
		S50	Using loss adjusters in parallel fashion	
		S51	Assimilation of loss adjusters service hiring contracts	
		S52	Having second internet service provider to avoid service interruption	
		S53	Development of a systematic approach for liaising with adds service providers	

The process of strategy setting for XYZ has resulted in identification of 53 strategies which have been mentioned in table 3. These strategies highlight the company approach to each major and minor category of the company strategies. Definitely, the strategies are set to achieve the company's objectives. If any strategy is wrongly selected and defined, the respective company objectives will be faced with some sort of deviations, i.e. the risk. In fact, the company objective is affected. These strategies are the points which have elements of uncertainty and something

might go wrong, i.e. where the sources of risks might exist. Thus, the proposed ORM can be applied to this process of strategy setting.

V. Conclusions

In line with the European Solvency II requirements, effective RMS is essential for an insurer's sound corporate governance. OR is one of the main categories of risk which require proper RM. ORs are those risks associated with processes, people and systems. ISO 31000:2009 as the Standard guideline for RM can effectively be used for the purpose of ORM. For this reason a conceptual model was introduced in Fig. 6. The model was tested by a typical strategic planning process selected from an anonymous insurance organization.

The effectiveness and efficiency of this model and its positive contribution to higher organizational performance shall be validated and verified. This is left as a suggestion and proposal for future studies.

VI. Bibliography

1. AIRMIC, ALARM, ARM, M.D., 2010. A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000.

2. Alhawari, S., Karadsheh, L., Nehari Talet, A., Mansour, E., 2012. Knowledge-Based Risk Management framework for Information Technology project. Int. J. Inf. Manag. 32, 50–65. doi:10.1016/j.ijinfomgt.2011.07.002

3. Bruckner, R., List, B., Schiefer, J., 2001. Developing requirements for data warehouse systems with use cases, in: Proc. 7th Americas Conf. on Information Systems. pp. 329–335.

4. Carbone, T.A., Tippett, D.D., 2004. Project risk management using the project risk FMEA. Eng. Manag. J. 16, 28–35.

5. Cule, P., Schmidt, R., Lyytinen, K., Keil, M., 2000. Strategies for heading off IS project failure. Inf. Syst. Manag. 17, 1–9.

6. Del Cano, A., de la Cruz, M.P., 2002. Integrated methodology for project risk management. J. Constr. Eng. Manag. 128, 473–485.

7. ISO 9004, 2009. Managing for the sustained success of an organization — A quality management approach.

8. ISO 31000, 2009. AS/NZS ISO 31000:2009 Risk management— Principles and guidelines.
ISO Guide 73, 2009. Risk management — Vocabulary.

9. Miles, F.M., Wilson Jr, T.G., 1998. Managing project risk and the performance envelope, in: Applied Power Electronics Conference and Exposition, 1998. APEC'98. Conference Proceedings 1998., Thirteenth Annual. pp. 247–253.

10. Ni, M., McCalley, J.D., Vittal, V., Tayyib, T., 2003. Online risk-based security assessment. Power Syst. IEEE Trans. On 18, 258–265.

11. Olsson, R., 2008. Risk management in a multi-project environment: An approach to manage portfolio risks. Int. J. Qual. Reliab. Manag. 25, 60–71.

12. Project Management Institute, 2013. A guide to the project management body of knowledge (PMBOK guide).

13. Risk_Management_in_the_Insurance_Industry_and_Solvency_II.pdf, n.d.

14. Segismundo, A., Miguel, P.A.C., 2008. Failure mode and effects analysis (FMEA) in the context of risk management in new product development: A case study in an automotive company. Int. J. Qual. Reliab. Manag. 25, 899–912. doi:10.1108/02656710810908061

VII. APPENDICES

Table A. Identification checklist for small businesses' risks

Small Businesses Risks
1) Financial – includes cash flow, budgetary requirements, tax obligations, creditor and debtor management, remuneration and other general account management concerns.
2) Equipment – extends to equipment used to conduct the business and includes everyday use, maintenance, depreciation, theft, safety and upgrades.
3) Organizational – relates to the internal requirements of a business, extending to the cultural, structural and human resources of the business.
4) Security – includes the business premises, assets and people. Also extends to security of company information, intellectual property, and technology.
5) Legal & regulatory compliance – includes legislation, regulations, standards, codes of practice and contractual requirements. Also extends to compliance with additional 'rules' such as policies, procedures or expectations, which may be set by contracts, customers or the social environment.
6) Reputation – entails the threat to the reputation of the business due to the conduct of the entity as a whole, the viability of products/services, or the conduct of employees or others associated with the business.
7) Operational – covers the planning, daily operational activities, resources (including people) and support required within the business that results in the successful development and delivery of products/services.
8) Contractual – meeting obligations required in a contract including delivery, product/service quality, guarantees/warranties, insurance and other statutory requirements, non-performance.
9) Service delivery – relates to the delivery of services, including the quality of service provided, or the manner in which a product is delivered. Includes customer interaction and after-sales service.
10) Commercial – includes risks associated with market placement, business growth, product development, diversification and commercial success. Also to the commercial viability of products/services, extending through establishment, retention, growth of a customer base and return.
11) Project – includes the management of equipment, finances, resources, technology, timeframes and people involved in the management of projects. Extends to internal operational projects, business development and external projects such as those undertaken for clients.
12) Safety – including everyone associated with the business: individual, workplace and public safety. Also applies to the safety of products/services delivered by the business.
13) Stakeholder management – includes identifying, establishing and maintaining the right relationships with both internal and external stakeholders.
14) Client-customer relationship – potential loss of clients due to internal and external factors.
15) Strategic – includes the planning, scoping, resourcing and growth of the business.
16) Technology – includes the implementation, management, maintenance and upgrades associated with technology. Extends to recognizing critical IT infrastructure and loss of a particular service/function for an extended period of time. It further takes into account the need and cost benefit associated with technology as part of a business development strategy.

Table B. Risk registration form

Phase no.	Phase name	Activities	Risk sources	Likely consequences	Action

Table C. Risk assessment form

IDENTIFICATION												EVALUATION				
Row	Risk	Source of the Risk (thing with potential to harm or assist)	What can happen (consequences)	How can it happen (cause for hazard to occur)	When & Where could the Risk occur	Business Goals/Objectives impacted by Risk	Assumptions & key variables used to assess risk	Business Process	Category	Link to Document	Document Type	Existing Controls	Assessment of Existing Controls	Consequence	Cost of Consequence (if known)	Likelihood	Risk Priority

Table D. Risk treatment and action plan

Risk number	Treatment number	Risk	TREATMENT / ACTION PLAN							Monitoring		ONGOING REVIEWS			
			Action	Possible Treatment Options	Result of Cost/Benefit	Action Type	Responsibility	By When	Residual Risk Rating	Key Risk Indicators	Reporting/Monitoring	Last Reviewed	Review Frequency (# Months)	Next Review Due	Responsibility

Table E. Risk reporting

		Assessment of Existing Controls				
		Adequate	Opportunities for Improvement	Inadequate	No Assessment	Totals
Risk Priority	V High					
	High					
	Medium					
	Low					
	Totals					

Table F. Risk likelihood and consequence

		Consequence					
		Catastrophic	Major	Moderate	Minor	Negligible	Totals
Likelihood	Almost Certain						
	Likely						
	Possible						
	Unlikely						
	Rare						
	Totals						

Color Code
V High
High
Medium
Low