International Business Research; Vol. 6, No. 1; 2013
ISSN 1913-9004 E-ISSN 1913-9012
Published by Canadian Center of Science and Education

Operational Risk Management for Insurers

Maria Isabel Martínez Torre-Enciso[1] & Rafael Hernandez Barros[2]

[1] Departamento de Financiación e Investigación Comercial, Universidad Autónoma de Madrid, Spain

[2] Departamento de Economía Financiera y Contabilidad III, Universidad Complutense de Madrid, Spain

Correspondence: Rafael Hernandez Barros, Departamento de Economía Financiera y Contabilidad III, Facultad de Ciencias Económicas y Empresariales, Universidad Complutense de Madrid (Campus de Somosaguas), 28223 Pozuelo de Alarcón (Madrid), Spain. E-mail: rjhbarros@ccee.ucm.es

Received: July 14, 2012 Accepted: August 3, 2012 Online Published: December 7, 2012

doi:10.5539/ibr.v6n1p1 URL: http://dx.doi.org/10.5539/ibr.v6n1p1

Abstract

Insurance companies face many risks, which should be managed, but their core competences and main contribution to society is to accept the risks underwritten by businesses and individuals, hence the strategic importance for citizens and governments that insurers protect their assets and revenues, and that policies and scientific methods are established to ensure a minimum financial solvency and the continuity of its operations. Operational risk is increasingly important in the management and corporate governance of insurance companies, which increasingly have greater implications and interactions with the other risks that this insurers face, such as market or credit risks. The management and analysis of operational risk is a necessary activity for insurers, presenting many opportunities for development and a major field of study on conceptual and practical issues due to the particularity and complexity implied in this type of risk. The new European regulation, Solvency II, will inexorably increase the need of an effective management of operational risks and the development and implementation of structured methodologies for its analysis. It is also reviewed the classical technique of modeling, Value at Risk (VaR), and other methodologies for the analysis and quantification of operational risk for insurers.

Keywords: risk management, insurance, operational risk, solvency II

1. Introduction

Given the current situation of operational risk, the purpose of the paper is to explain why operational risk is increasingly important in the management of insurers to estimate the need of solvency capital. The paper shows also that the methodology process to estimate the capital charge is a key issue to help management and risk managers to understand the organization better and analyze the risk they are exposed to.

From a macroeconomic perspective, the economy of a state depends on the processes of public administration, industrial, infrastructure and services sectors to operate efficiently and smoothly. When this is not the case, for example, due to a natural disaster or an industrial or a major financial crisis, it is paid a price in the form of lost economic competitiveness, increased operating costs, reduced growth expectations, unemployment or even a recession.

With respect to the point of view of microeconomics, individual companies also face the risk that their activities and processes are interrupted unexpectedly or failing to achieve the expected results (Ramanujam, 2003). In particular, the recent financial crisis has focused attention on all levels about the importance of risk management (Raei, Ahmadinia & Hasbaei, 2011). In particular, boards of directors have begun to consider and evaluate risk management as an important element of the strategy of sound corporate governance and as a tool to protect the interests of shareholders.

The operational risk management mission is to identify, analyze and mitigate the different risks business operations are exposed to, in which we can identify two main parts that can be found in the organizations, individually or interrelated:

1) The existence and integrity of management and operational controls of the company, with appropriate cultural settings to satisfy the current legislation on job security, data, environment and others, and to prevent fraud.

2) The ability to fulfill the promise made to customers, doing the activities and processes needed to serve

customers and meet with other stakeholders, including shareholders, employees or suppliers.

In this context, management has always paid more attention to the service and the smooth of efficient operations of the company (Siddiqui & Sharma, 2010) than to the strategic part of the management of operational risks, such as its alignment with the overall growth objectives and profitability. And this is beginning to change, as it is proving every day that the consequences of not adequately manage the risks of operations beyond the direct economic losses, such as legal penalties or damage the reputation of the company for shareholders and customers, could lead to a reduction in market share and brand value.

In addition, the attention that failures due to poor operational risk management are receiving in recent years in the press and other media companies is causing an increasing concern in organizations about the importance of managing and controlling such risks; especially when changes in the economic, social and technology world are becoming faster, such as globalization, technological developments, competitive environments or legislative requirements.

These ongoing changes have transformed the way how managers perceive risks, because organizations that achieve success in this environment of uncertainty are those which give more importance to innovation, risk taking and entrepreneurship, and strive to develop a culture of change acceptance and adaptation in order to keep improving. Economic, social or personal advancement mean taking some kind of risks, and this progress not only refers to the ultimate success of achieving a goal, but to the skills and experience acquired during the process that will help to continue progressing.

Moreover, it does not seem very reasonable to be overly defensive in the management of risk, a danger which in turn can lead to the elimination of opportunities the company's ability to innovate and create value. This type of defense policy is the common denominator in risk management in most economic sectors, the traditional anti-fraud, security and theft, or breach of law and asset protection, which on the other hand, are also important to manage, but they are not the essential ones: targeted at seeking opportunities and income.

The methodology used has been a conceptual analysis of the current state of affairs, based on the analysis of available bibliography: A thorough revision was made of the regulatory framework, due to the new insurance regulation in Europe, Solvency II; a study of the risks insurers face in each phase of the insurance business process was completed, including an approach to the main known practices to control it; then a revision of the definition for operational risk was needed, analyzing its nature and its expected loss behavior; and finally, a revision was prepared of the models used in financial literature for the actuarial financial analysis of operational risk.

2. Background

Operational risk is not a new risk, in fact is the first risk that an insurer has to manage, even before signing the first policy. However, the idea that operational risk management is a discipline with its own organizational structure, tools and processes, like credit or market risks, is new and has evolved considerably lately (Hernández & Martínez, 2012b).

In 1998, the Committee on Banking Supervision published an advisory work related to operational risk, enabling it to become an accepted part of good risk management practices in modern financial markets. According to this study, the major types of operational risk include failure of internal controls and corporate governance. Failures that can lead to financial losses through error, fraud, or failure in the implementation of obligations in a timely manner or that could compromise the existence of the entity in some way. This could include all levels of the organization that exceeds its authority or conduct unethical and unsafe practices. Other aspects of operational risk include systems failures in information technology, or events such as fires and other disasters.

Most financial institutions allocate the responsibility for managing operational risk to managers in the business units, so it is necessary to develop the incentive structures and processes for best practices. Those systems are being incorporated into the overall process of internal evaluation, and requiring to those responsible for the business units and losses the details of the results of corrective actions undertaken.

Operational risk management is in the early stages of development. Awareness of operational risk as a separate risk category is being driven by most accounting firms, which are beginning to include comments from risks in their annual audit reports. On the other hand, only a few financial institutions now measure and report their risks on a regular basis, although many are monitoring the operational performance indicators, analyze the experiences of loss and monitor the audit and regulatory ratings. Unlike market risk, and perhaps credit risk, operational risk factors are mostly internal, and there is still no clear mathematical or statistical relationship between individual risk factors and the likelihood and size operating losses (revenue volatility).

Experience with large losses is infrequent, and many organizations do not have their own historical series of operating losses and causes of them. And models are developed on a very limited data series and with similar risk factors, such as audit ratings, self assessment controls, operational indicators as volume and number of errors, the experience of losses or revenue volatility.

One potential benefit of a formal operational risk approach is, where possible develop enough incentives for business units managers to adopt sound risk management practices through capital allocation, performance reviews and other mechanisms. In general, insurers and financial institutions are convinced that the programs of operational risk management protect and enhance shareholder value, because is a distinctive internal function with its own processes, structures, tools, statistics and risk mitigation strategies.

This situation is contributing to develop a formal process and an improved transparency of one of the oldest forms of risk, due to the following circumstances, among other things:

1) The creation of programs for managing operational risk is due to a combination of management commitment, the need to understand the risks of the company, a perceived increase in exposure to operational risk and a regulatory interest.

2) There is a consensus on the operational risk definition, which will be later described.

3) Though Operational Value at Risk (OpVAR) is considered the generally accepted tool for decision-making, new methodologies and research are continuously emerging towards quantifying the capital required to cover operational risk.

4) After the development of market and credit risk management, it is being perceived an increased attention by underwriters to an integrated risk management approach, which includes operational risk.

5) The existence of an increased interest by regulatory authorities to quantify operational risk, such as the European regulation Solvency II.

3. Concept and Nature of Operational Risk

Many organizations have their own definitions of what operational risk is, but there is general agreement on what was established by New Basel Capital Accord II: the risk of loss, direct or indirect, caused by inadequate internal processes and/or wrong, people and systems or by external events. More specifically for the insurance industry, operational risk, by the standards of Solvency II (Directive 2009/138/EC), is the risk of loss arising from inadequate or failed internal processes, personnel or systems or from external events, and includes legal risks, but not risks arising from strategic decisions and reputational risks (Figure 1).

These definitions have a general positive spirit that can be tailored to the particular circumstances of each company. An important distinction is that the definition focuses on the source of losses, but that does not express the major risk factors operating in most companies, and can facilitate the exchange of information. We also understand that this definition does not attempt to reach those risks that are not included or have not been determined either in the definition of other risks, including market and credit risks. But the most important feature of this definition is that it focuses on the impact of operational losses.

According to the advisory report of the Committee on Banking Supervision Basel II (2005) above mentioned, until that time it did not exit a generally accepted universal definition of operational risk. The most widely accepted definition of operational risk was that risk that was not market or credit risk. Other institutions have defined it as the risk of loss from various types of human or technical errors, and others have associated it with business interruption and legal and administrative risks. In contrast, all the institutions participating in this study (Committee on Banking Supervision Basel II advisory report) share the view that there is some kind of union or axis between the different risks of a company, such as market, credit and operational risks. In particular, an operational problem with a business transaction, as for example an error in recording data from a client, can create either a credit risk or a reputational one if it affects the client personal data.

While many organizations believe that technology risk is part of operational risk, some consider it as a separate category with its own risk factors. In addition, most senior managers view operational risk as a general back office risk, although the mix of risks and their relative magnitudes can vary for each business unit. Operational risk is sought in the business areas with a high volume of business or operations, which have more structural changes or have complex support systems, as in policy administration and receipt collection activities.

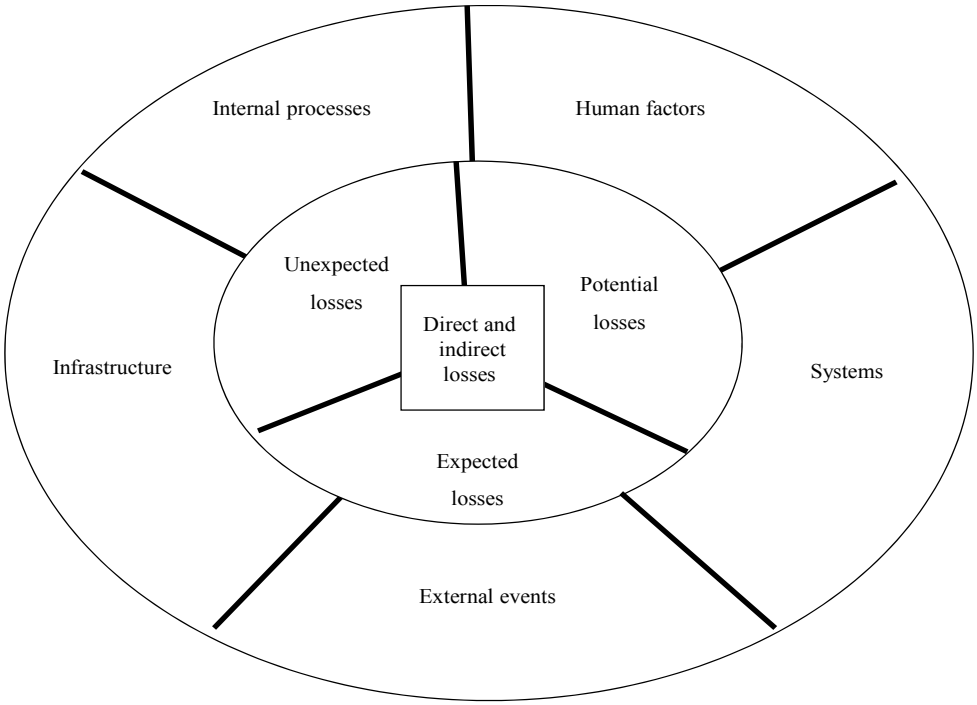

Figure 1. Definition of operational risk

Description: Interpretation by the authors of the definition of operational risk according Solvency II (Directive 2009/138/EC).

The operational risk of a company comes from the influence and interaction of internal and external events in people, processes and technology applied to business processes of an organization. Since each entity is unique in the way of combining human resources, processes and technology, is actually a very complex task creating a single generic definition of what constitutes operational risk. The former existing definitions of operational risk are not clear and are focused primarily on the negative aspects of risk, including the potential that, for any reason, business processes were interrupted resulting in a direct or indirect financial loss.

The events that trigger losses may have been caused by several factors, including failures in information systems, processes and controls, human error or fraud, or unforeseen natural disasters. Direct losses refer to losses in current income, while indirect losses relate to potential revenue, for example, due to impediments to business expansion or reduction in customers due to reputational issues. Such definitions refer to historical facts and their uses are limited to prevent future losses or to anticipate threat to organizations. Less traditional operational risk definitions, but potentially more strategic, incorporates a positive view of risk: instead of considering the risk solely as a financial loss due to exposure to market or credit risk, operational risk includes the consideration of a failure in the process or strategic investment decisions to optimize revenue or financial performance; and introduces the concept of opportunity cost.

From a theoretical and academic point of view, it is desirable to clarify the discussions about operational risk and to identify and differentiate all definitions of risk within a general framework and avoid the overlapping with other well-defined risks, including market and credit risk. By analyzing recent losses, negative developments are typically assigned to the causes and impacts. Causes could be the unwanted deviations from an expected result, and the impacts would be the risk, as normal losses incurred can be expressed in monetary terms. Many definitions do not distinguish between causes and impacts, which makes complex their identification and differentiation. This is especially problematic for operational risks, as the process of building databases of losses requires a structure of categories of those losses.

The quantitative analysis based on a mixture of definitions has also little sense, because it aims at defining the losses as market risks. In this context of relationships between causes and impacts, a good definition of operational risk is essential, as the fundamental principles of internal control and segregation of functions are omitted in these cases.

For the purpose of this research, we use the operational risk definition of Solvency II mentioned above, which distinguishes between direct and indirect impacts of the causes of operational risk. The impact may manifest

itself as a market risk, resulting in a loss or gain. This is based on the assumption that it is possible to identify the causes of operational risks, such as an unexpected loss due to internal errors, assessments of situations, strategy and external events incorrectly. Poor supervision of operational risks can result in losses of other risks, which could have been prevented by internal control systems and a culture of appropriate management.

Direct impacts affect, at the time of its occurrence, directly to the profit and loss account and balance sheet, but indirect losses will become lower values of expected cash flows in the future. A concrete example is the claims made by clients with a very high risk profile due to errors in the underwriting process for a period of time. This will likely diminish the benefits of the insurer due to an increase in accidents, which can affect their ratings and market value.

We can conclude that any definition of operational risk is controversial. The definition of Solvency II, though includes material exposures to legal and regulatory risk arising out of business development, excludes strategic and reputational risks.

3.1 Reputational Risks versus Operational Risks

In contrast, although reputational risk has been considered until now as an integral part of the definition of operational risk, it is not presumed that the definition of operational risk is amended including reputational risk as a component of it. This is important for the financial sector because reputational risk is one of the threats to these companies, because the good name is very often a key intangible asset. Damage to brand and reputational risks are more complicated to manage and overcome, as they are not solved with the payment of a fine or compensation.

Much global insurers have an extensive group of stakeholders, which can be summarized under the following headings:

1) Shareholders, who provide capital.

2) Employees, who provide intellectual capital.

3) Customers, who provide income.

4) Suppliers, who provide specialized services or products.

5) Business alliances, facilitating contacts and / or ways to access new markets.

6) Society in general, which provides the overall framework and technical, economic and legal infrastructure, where companies could develop and prosper.

In recent years, these stakeholders have focused primarily on operations, improving their ability to analyze and judge them, but a new environment have emerged in the workplace, and in the society in general, behaviors that should be cared because could lead to reputational events, such as:

1) Sexual harassment.

2) Racial discrimination, age, religion, etc.

3) Environmental issues.

4) Sale or misleading customer relationship or lack of ethics and honesty.

The result is that companies around the world are at risk of their reputation, being far more lasting this damage in the market than last news in the business press. It may affect the way that customers and other stakeholders conceived the organization and the products or services provided. Being able to affect sales estimations or may never recover, as more and more situations or experiences of this kind show that unethical behavior negatively affects the value of the company, whether it be the market value, brand value or attractiveness to work in it.

Several factors may increase the risk of damage to the reputation of the majority of companies: the extension of markets and globalization, both in existing areas as new ones, the new social interpretations of what constitutes ethical behavior, greater ease of access to information sources and the growing importance of media and pressure groups.

Operational risk management can help control and mitigate these risks. Companies that incorporate management or leadership positions in the area of governance will enjoy competitive advantages. For example, the issue about transparency of information has rapidly become a positive attribute in the business and financial areas, but for being accepted by senior governing bodies, they need to have full confidence in the integrity on the risk operational controls.

Two factors that are completely linked, considering reputation as a strategic asset, are building confidence in the

strategy and capabilities to deliver products and services. All this only serves to emphasize the importance that reputational risk is becoming an area of interest for the company and shareholders. In addition, quantifying and capitalizing reputational risk is not an easy task, and usually does not fit well with the quantification and capitalization of operational risk, such as technological or system failures or errors in making payments. Being this one of the reasons why it has been concluded that the reputational risks should not be included within the operational risk.

3.2 From Risk to Capital

There are not any measurement techniques or capital models in the world which reduces operational risk by them. This is done in coordination with sound and culturally established management processes in organizations. These models help companies to reduce capital requirements, enabling the excess of money being use in other more profitable investments, while retaining exposure to the risks that may affect the ability to generate future income.

Most of the risks in the financial industry can be divided into the following:

1) Expected losses, covered by provisions.

2) Unexpected losses, which are covered with the minimum required capital and the reserves of the company.

3) And catastrophic losses, which have to be prevented by internal controls, risk transfer schemes as insurance instruments or alternative risk transfer.

The problem lies in clarifying the rules on operational risk capitalization, as it is rather vague to explain the proportion and types of operational risk that fall into each category, and because the boundary between them move as the industry evolves. It is important to note that the quantification and measurement of operational risk is only a tool among others, in the establishment of a system or risk management program viable and complete.

3.3 Operational Risk Categorization

To understand the components of internal operational risk, and one of the main tools for implementing a global operational risk management in an insurance company, it is essential to use a database that records the loss of such risks, which need to be sorted to obtain a homogeneous data and to allow further analysis. The ORIC (Association of British Insurers, 2012) loss event type classification for operational risk (Table 1), a consortium database for insurers, manages and collects the external database of operational risk for insurers that exists currently in the UK, and it is used as standard for the classification of operational risk events.

Table 1. Loss event type classification (insurance version)

Event-Type Category (Level 1)	**Categories (Level 2)**
Internal Fraud	Unauthorized Activity
	Theft and Fraud
External Fraud	Theft and Fraud
	Systems Security
Employment Practices and Workplace Safety	Employee Relations
	Safe Environment
	Diversity & Discrimination
Clients, Products & Business Practices	Suitability, Disclosure & Fiduciary
	Improper Business or Market Practices
	Product Flaws
	Selection, Sponsorship & Exposure
	Advisory Activities
Damage to Physical Assets	Disasters and other events
Business Disruption and System Failures	Systems
Execution, Delivery & Process Management	Transaction Capture, Execution & Maintenance
	Monitoring and Reporting
	Customer Intake and Documentation
	Customer / Client Account Management
	Trade Counterparties
	Vendors & Suppliers

Description: Loss event type classification (insurance version), from the Consortium database ORIC for insurers (Association of British Insurers, 2012).

3.4 Definition of Operational Loss Events

To understand the scope of operational risk management, and the definition stated by Solvency II, it should be considered what it is included as operational risk. It is therefore necessary to define and clearly identify what is a loss event and its consequences.

1) Cause: Why did it happen?

2) Event: What happened?

3) Result: How much did it cost?

Operational event is considered as the event that may cause an operating loss, so it is necessary to clearly identify its consequences are measured, i.e. the impact of an event, and they are all extra costs resulting from the operational events losses not incurred in the absence of the event. Among these costs are included refunds, loss of revenue, losses (reduction in value of financial assets), regulatory actions, loss or damage to assets and legal contingencies. Excluding the following, not considered direct costs of an operating event: preventive measures taken in connection with the event, improved controls, investment plans, income generation stopped, lost reputation or opportunity costs.

3.5 Nature of Operational Events

When identifying operational losses, it can be determined by two parameters. On the one hand, in terms of their impact, severity or amount of loss, and on the other hand, depending on how often the event repeats itself over a period of time or, put in another way, the probability that an event occurs. Thus, the losses can be categorized according to the scheme in Figure 2.

The nature of operational events is a function of its occurrence (frequency) and of its impact (severity):

1) Recurring events: High frequency and low impact type. It is the best known part of operational risk, such as fraud in reporting claims.

2) Non-recurring events: Low frequency and high impact type. It is the most dangerous part of operational risk, like a fire or destruction of one of the buildings of an insurance company.

Internal loss data are a critical element in designing a model of internal measurement, since they best represent the business structure, the control systems and the culture of each organization. In this sense, the main difficulty in the management of operational risk is in the unavailability of internal databases with which to approximate the variables used in the model. Therefore, Solvency II rules allow, as does Basel II, to complete this data with the use of external databases in order to add information about events, mainly low frequency and medium or high severity, which probably has not been experienced by the insurer, but it is still exposed.

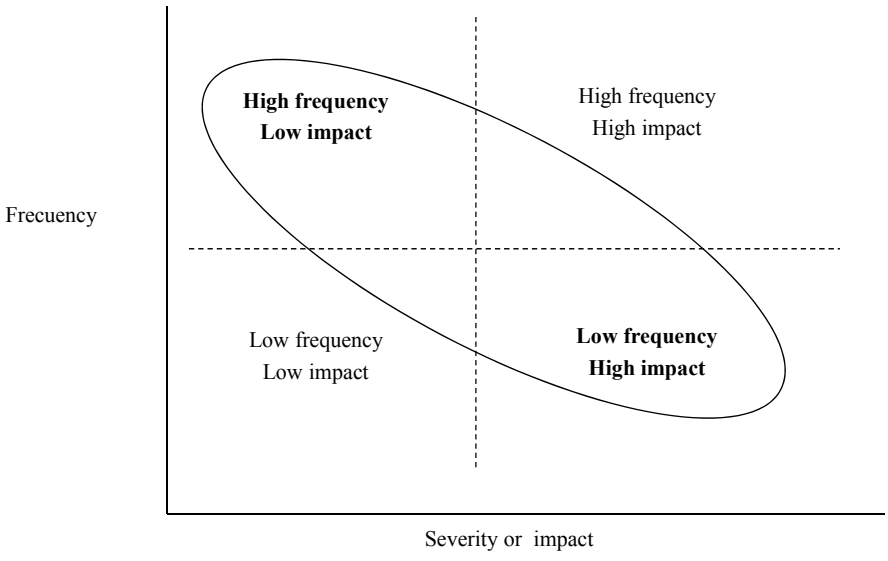

Figure 2. Categorization of losses Combinations

Description: Combinations of frequency and severity for operational risk events (Jordan, De Fontnouvelle, Dejesus-Rueff, &Rosengren, 2003).

4. Organization and Control of an Integrated System of Operational Risk Management

COSO Report, published in the U.S.A. in 1992, was a response to the concerns posed by the diversity of concepts, definitions and interpretations of existing internal controls. In the report are presented the results of the research conducted during more than five years by the working group that the Treadway Commission, National Commission on Fraudulent Financial Reporting, established in the United States in 1985 under the acronym COSO (Committee of Sponsoring Organizations). The group consisted of representatives of several international accounting and auditing organizations, and the report was undertaken by Coopers & Lybrand.

Internal control is defined (Coso, 2004) as the process carried out by a company in order to assess, with reasonable assurance, the activities into three main categories: Effectiveness and operational efficiency, reliability of financial reporting, and compliance with policies, laws and regulations. This definition completes some fundamental concepts such as that internal control is a process, i.e. a means to an end not an end in itself, that is carried out by persons acting at all levels, and therefore is not just a series of organizational and procedural manuals; internal control only provide a reasonable degree of security, not the total security; and that it is designed to facilitate the achievement of a number of objectives. In this context, internal control has five components that can be implemented in all the insurers in accordance with the characteristics of each:

1) Environment of control

2) Risk assessment

3) Control activities (policies and procedures)

4) Information and communication

5) Supervision

On the other hand, to be effective operational risk management, it should be integrated into the organization at all levels, both in the policies and culture of the company as in its structure and processes. So far, this risk systematically has been difficult to manage, as the business units responsible dealt with those who threatened them directly, without approaching it from the holistic view across the organization, and also due to a lack of proper structures and policies.

To establish an operational risk management unitwithin an organization, it should be taken into account several factors or drivers, as the institutionalization of procedures to ensure that the risk is properly managed, train and aligned staff to common goals, develop a culture of control, also including the establishment of dependency relations between roles and responsibilities.

A holistic approach to risk management needs an organization that makes possible to assess these mentioned variables simultaneously, both the most viewable or tangible (strategy, structure and support systems and processes) and the more intangible (shared values, staff, skills of the company or management style). Together, these factors determine the way in which an organization operates, and should consider all of them to be sure of their successful implementation: They are all interdependent, if a company fails to pay proper attention to one of them, all others could be affected as well. In addition, the relative importance of each may vary over time.

The problems caused by corporate governance in the last decade have increased the importance now attributed to internal control, which has become an essential business process. These recent corporate crises have accelerated efforts to find an effective system of self-regulation that will avoid such situations in the future, but also on the other hand, it is well understood that the focus of risk management on internal controls is not the right path towards a long term solution to these problems that risk raises, supporting decisions in the scope of strategic management and in the sustainability of the competitive advantage.

That is, although the new practices and interest in internal control are very positive for organizations, they should be regarded as a tool for making informed decisions about risk on the part of managers, and to balance risk and reward. Therefore, the idea to convey is that the implementation of a risk management system provides a means for organizations to be better able to achieve their business objectives, and that its organizational variables or drivers facilitate strategic decisions without being overly focused on the control and supervision. Internal audits, for example, have traditionally been very focused on financial risks, leaving aside the general business and operational aspects. It also tends to be understood internally in a less positive way, as a police officer or control, rather than a tool to improve the risk management for the company.

Adopting some risk management systems of this type, apart from being a competitive advantage, can improve the external image of the company. The institutions that are able to demonstrate that they have an appropriate risk management system, have a more attractive profile to investors, soon becoming an important element of

their market value, since it assumes that you an analysis and risk management of new projects and strategies for growth or sale have been completed. In this sense, corporate governance can be considered as a control system that tries to balance the entrepreneurial management energy and their associated risks, developing an effective control by aligning the interests of management with those of shareholders and the other stakeholders of the company, allocating resources (financial, human or otherwise) as well to those areas which capital will be used more efficiently, and managing market competition.

5. Risk Management Internal Models in the Context of Solvency II. Operational Risk and VAR

Internal models for risk management have been around for several years, but only recently more advanced models are appearing, which initially were usually used by large insurers, especially those operating in several countries, and reinsurers. Although these models were developed in the absence of regulation in this regard, they helped to improve risk management standards in general and to shape a new regulatory framework (Solvency II) which would assist to better understand the risks of the insurance industry as a whole, in a world that is increasingly more complex and globalized, with larger risks, closely interconnected.

In any case, risk management for insurance companies should cover the key elements of the business cycle, as well as a proper management of risks exposed, as expressed in Figure 3, in which it is linked each phase of the business cycle - from the cover note to claims management, through the policy administration and management by the insurer – to a particular risk. For example, in the investment phase of the insurance premiums, there is investment risk, and at all stages of the process, it is implicit operational risk.

Insurance industry has traditionally used the same types of quantitative models to calculate and price provisions, but have also been used to calculate solvency and capital requirements, focusing mainly on the estimation of expected valuesrather than the subsequent deviation of those expected values (Tripp, 2005). Moreover, they do not cover all the risks to which insurers are exposed. Recently, due to advances in information systems and telecommunications, these models have been richer and more complex, incorporating all risks into one, and whose objective is the efficient allocation of capital.

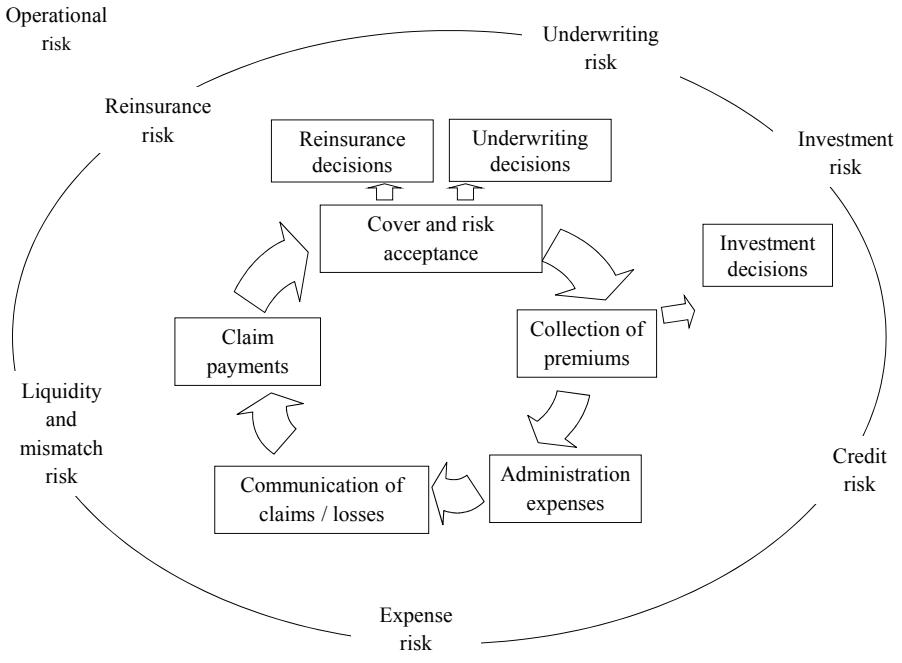

Figure 3. Insurance business cycle vs. risks

Description: Business cycle of insurance companies linked to the risk they face. Compiled by the authors.

5.1 Integration of Internal Models in the Regulatory System: Solvency II

The existence of an internal financial model ensures a culture of risk supervision across the company, forcing it to make inventory of all potential sources of risk, assessing the relative importance of all the risks (Chorafas, 2004). In addition, the internal models propose a definition and measurement of capital requirements according

to the characteristics of the activity of the company. However, these models produce a number of difficulties to the supervisor to be taken into account, as the model does not provide an exact figure of the capital needed, but just study extreme events whose probability of occurrence is low, and that the assessment of risk internal models may not be enough for their evaluation. Therefore, the use of internal models involves new burdens and difficulties both for insurance companies and to the supervisory authority.

The developments of greatest relevance and impact on the insurance sector, referred to in the Solvency II Directive, relate mainly to the management of different risks, capital requirements for solvency and the establishment of monitoring criteria. In line with recent developments in risk management, actuarial science and recent developments in the financial sector, Solvency II has adopted a risk-based approach that encourages a proper economic assessment and risk management from insurance and reinsurance companies.

With regard to solvency capital requirements, it is required for insurers and reinsurers to maintain a level of equity that enable them to cope with significant losses. Thereby providing citizens who take out insurance some guarantees that claim payments will be met at maturity. In accordance with good risk management practices, the economic capital solvency is estimated based on the risk profile of each entity, taking into account the particular techniques of risk mitigation and diversification of the company. To enable all companies to assess their economic capital and thus reflect the risk profile of the insurers, Solvency II sets a simple standard formula for calculating the solvency capital to ensure a minimum level below which should not descent the financial resources. As an alternative to the calculation of capital according to the standard formula, also establishes the possibility of the use, under specific conditions and approval of supervisor, of internal complex or partial models, so that insurers can achieve a reduction in capital requirements.

5.2 Models for Operational Risk Analysis of Insurance Companies

From the study of models used in financial literature for the actuarial financial analysis of operational risk, it can be concluded that the models most used are the probabilistic ones, which are more related to financial and actuarial calculations traditionally associated with the financial and insurance sector (Hernández & Martínez, 2012a). Of these, highlight Value at Risk (VaR), extreme value theory and stress testing and scenario analysis models as the most common and easiest to implement in practice. As for deterministic models, Bayesian networks stand out for its novelty and calculation complexity; regarding econometric models, there was not found literature on its application to operational risk.

Operational value at risk (OpVaR) concept arises from the application of VaR to the context of operational risk, since it also studies the percentile of a loss distribution, now arising from operational losses or failures and not by variations in financial asset prices.

OpVaR can be defined as an amount, expressed in monetary units, which provides information on the minimum potential loss that may incur a certain business unit or company, by operational risk type, within a given time and at a certain level of statistical confidence. The main specifications that determine a correct definition of OpVaR are:

1) Timeframe. OpVaR is a statistical estimation referred to a period of time, usually one year.

2) Statistical confidence level. In general terms, it is used a variation of intervals between 95 percent and 99 percent, this allows defining the probability of loss associated with a time horizon. To calculate the capital requirements of an organization, the selection of the level of confidence will depend both on the degree of risk aversion, and the cost of exceeding the figure OpVaR. That is, the greater their risk aversion, or higher cost of capital, the greater its need for capital, and therefore the confidence level of estimation. For reference, Solvency II suggests a statistical confidence level of 99.5 percent for the calculation of regulatory capital.

3) A company or business unit OpVaR, should be madein a reference currency, such as Euros or Dollars.

Therefore, given the current state of research on the subject, and a clear position on operational risk models by Solvency II, the classical model VaR is positioned as a common measure susceptible of universal application to a variety of risk categories and business lines, and because the result is expressed as a figure in monetary units, which facilitates internal and external comparisons and the possibility of obtaining a series of conclusions on its practical applicability to insurance companies in Europe.

6. Conclusions

Insurance companies face many risks, which have to be managed, but the complexity of these companies comes from the nature of their operations, which is to accept the risks underwritten by other entities or individuals. Hence the strategic importance for citizens and governments that they protect their assets and income and that

policies and structured scientific methods are establish in order to ensure a minimum financial solvency and the continuity of their operations.

Operational risk is increasingly important in the management and corporate governance of insurance companies. The different operations and processes of these organizations increasingly have greater implications and interactions with the other risks they face, such as market or credit risks. Management and financial analysis of operational risk is a necessary activity for insurers, presenting ample opportunities for development and a major field of study on conceptual and practical issues, since the particularity and complexity involved in this type of risk.

The new Solvency II regulation, structured on three pillars (financial requirements in accordance with the actual level of risk assumed by insurers, internal control mechanisms and market transparency and discipline), will inexorably increase the need for an effective management of operational risk and the development and implementation of methodologies for its analysis.

Finally, the need for a capital that faces the possible loss of operational risk is a reality that has been materialized with Solvency II rules. The classical technique of modeling VaR is, with no doubt, and with respect to other methodologies, the one that gets closer to the solvency goals, since it is a simple, reliable, well known and easily applicable tool. VaR model is also a reference for Basel II for the actuarial financial analysis of operational risk. On the other hand, as a criticism extended to all statistical methods, these techniques alone are a purely quantitative exercise, that somehow leaves pending the incorporation of the qualitative side to the management of internal risks.

References

Association of British Insurers. (2012). *Consortium database ORIC for insurers*. Retrieved from http/www.abi.org.uk

Basel Committee on Banking Supervision. (2005). *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework*. Basel Committee on Banking Supervision.

Chorafas, D. N. (2004). Operational risk control business opportunity and challenges for the insurance industry. *Geneva Papers on Risk and Insurance: Issues and practice, 29*, 87-101. http://dx.doi.org/10.1111/j.1468-0440.2004.00274.x

Coso. (2004). *Enterprise Risk Management*. Integrated Framework.Coso.

Directive 2009/138/EC of the European Parliament and of the Council, of 25 November 2009, on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II).

Hernández Barros, R., & Martínez Torre-Enciso, M. I. (2012a). Capital assessment of operational risk for the solvency of health insurance companies. *The Journal of Operational Risk*, *7*(2), 43-65.

Hernández Barros, R., & Martínez Torre-Enciso, M. I. (2012b). Operational losses for the capital charge of health insurers: Lessons from Spain. *The Geneva Papers on Risk and Insurance - Issues and Practice*, nº 37, 763-779. http://dx.doi.org/10.1057/gpp.2012.4

Jordan, J., De Fontnouvelle, P., Dejesus-Rueff, V., & Rosengren, E. (2003). Using loss data to quantify operational risk. Bank of Boston. *Working paper*.

Raei, R., Ahmadinia, H., & Hasbaei, A. (2011). A Study on Developing of Asset Pricing Models. *International Business Research, 4*(4), 139-152. http://dx.doi.org/10.5539/ibr.v4n4p139

Ramanujam, R. (2003). The Effects of discontinuous change on latent errors in organizations: The moderating role of risk. *Academy of Management Journal, 46*(5), 608-617. http://dx.doi.org/10.2307/30040652

Siddiqui, M. H., & Sharma, T. G. (2010). Measuring the Customer Perceived Service Quality for Life Insurance Services: An Empirical Investigation. *International Business Research, 3*(3), 171-186.

Tripp, M. H. (2005). Quantifying operational risk in general insurance companies. *British Actuarial Journal, 49*.