

MANAGING THE IMPACT OF OPERATIONAL RISK ON THE SOLVENCY OF INSURANCE COMPANIES

Festus M Epetimehin^{a, b}

^a Joseph Ayo Babalola University, Ikeji –Arakeji, Nigeria.

^b Actuarial Science and Insurance, Nigeria.

^a Corresponding author: fessy51@yahoo.co.uk

©Ontario International Development Agency ISSN: 1923-6654 (print)
ISSN 1923-6662 (online). Available at <http://www.ssrn.com/link/OIDA-Intl-Journal-Sustainable-Dev.html>

Abstract: Insurance companies face many risks, which should be managed. Though their core competences and main contribution to society is to accept the risks of businesses and individual and to protect their assets and revenues, they have 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 other risks, such as market or credit risk. 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. Making use of secondary data collected through library research, journals and analysis of reports, the paper reviewed the operational risks of insurance companies and their management for solvency. The new European regulation Solvency II if adopted will inexorably increase the need of an effective management of operational risks, the development and implementation of structured methodologies for the analysis and quantification of operational risk.

Keywords: Corporate Governance, Insurance, Operation risk Risk Management, Solvency II,

INTRODUCTION

One of the main obstacles facing organisations today is the risk of having their activities and processes interrupted unexpectedly or failing to achieve the expected results. In particular, the

recent financial crisis has focused attention on all levels about the importance of risk management. 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. (Di Renzo, et al., 2007)

The operational risk management mission is to identify, analyze and mitigate the different risk business operations are exposed to, in which we can identify two main parts that can be found in the organizations, individually or interrelatedly: (a) 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. (b) The ability to fulfil 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 and efficient operations of the company 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 the change that is proving every day that the consequences of not adequately managing the risk of operations beyond the direct economic losses, such as legal penalties or damage of the reputation of the company for shareholders and customers, could lead to a reduction in market share and brand value. (Chorafas, 2004)

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 organisation about the importance of managing and controlling such risk; especially when changes in the economic, social and technology world are becoming faster, such as globalizations technological developments, competitive environments, legislative requirement, etc.

These ongoing changes have transformed the way managers perceive risks, because organization 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.

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.

In 1998, the Committee on Banking Supervision in UK published an advisory work related to operational risk; enabling it to become an accepted part of good risk management practices in modern financial market. According to this study, the major types of operational risk include failure of internal controls and corporate governance. Failure 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 includes all levels of the organization that exceeds its authority or conduct unethical and unsafe practices. Other aspects of operational risk include system failures in information technology, or event such as fires and other disasters.

Adeleye, et al. (2004) observed that 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 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 of operating losses (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, structure, tools, statistics and risk mitigation strategies.

This situation is contributing to the development of a formal process and an improved transparency of one of the oldest forms of risk.

CONCEPT 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 system or by external event. More specifically for the insurance industry, operational risk, by the standard of Solvency II, is the risk of loss arising from inadequate or failed internal processes, personnel or system or from external events, and includes legal risks, but not risks arising from strategic decisions and reputational risks (Fig. 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 sources 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.

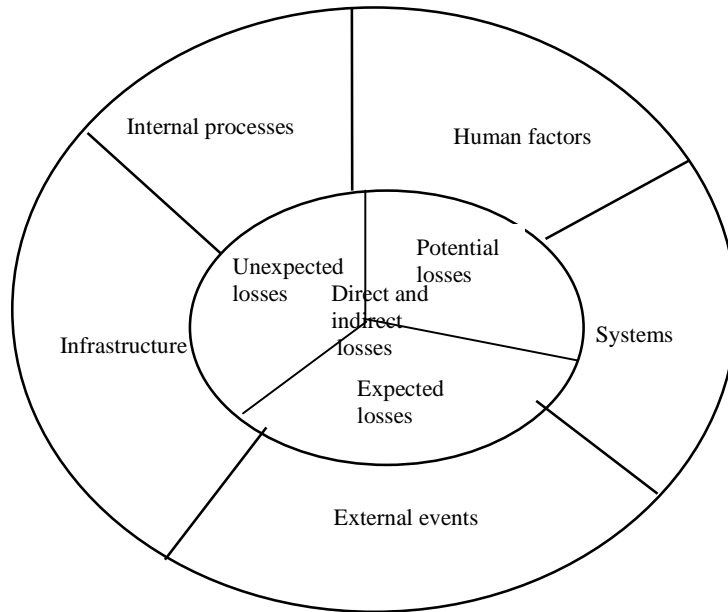


Figure 1: Definition of operational risk
Source: Compiled by the Author

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	Disaster 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

Source: Consortium database ORIC for insurers, obtained from the Association of British Insurers web page, www.abi.org.uk, Jan. 2010

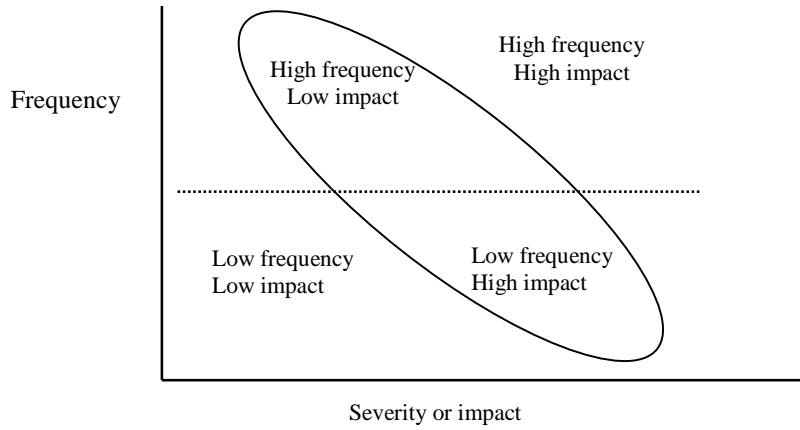


Figure 2: Combination of frequency and severity for operational risk events

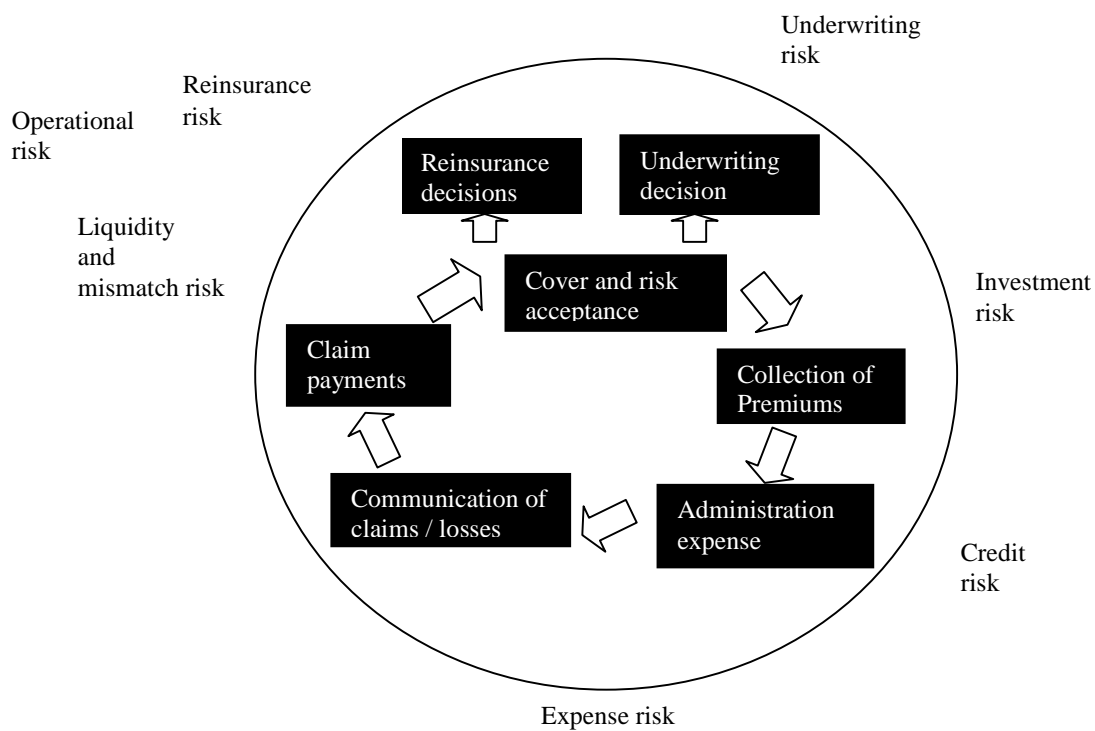


Figure 3: Insurance business cycle vs. risks
Source: The Author. 2012

There was no generally accepted universal definition of operational risk until the advisory report of the Committee on Banking Supervision, Basel II. 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 clients, can create a credit risk or a reputational one if it affects the client's 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. 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 system, as in policy administration and receipt collection activities.

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 organisation. 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 aspect of risk, including the potential that, for any reason, business processes were interrupted resulting in a direct or indirect financial loss.

The event that trigger losses may have been caused by several factors, including failure in information system, processes and controls, human error or fraud, or unforeseen natural disaster. 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 customer due to reputational issues. Such definitions refer to historical facts and their uses are limited to prevent future losses or to anticipate threat to organization. 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 impact, which makes complex their identification and differentiation. This is especially problematic for operational risks, as the process of building database of losses requires a structure of categories of those losses.

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 risk, 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 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.

From Risk to Capital

There are no measurement techniques or capital models which reduces operational risk by themselves. This is done in coordination with sound and culturally established management process in organisations. 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 risk in the financial industry can be divided into the following: (a) Expected losses, covered by provisions. (b) Unexpected losses, which are covered with the minimum required capital and the reserves of the company. (c) 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 type of operational risk 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.

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 homogenous data and to allow further analysis. The ORIC loss event type classification for operational risk (Table 1), a consortium database for insurers, 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.

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 (a) Cause: Why did it happen? (b) Event: What happened? (c) 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 and 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. (Alexander, 2003) Among these costs are included according to Bellando, (2001) 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 control, investments plans, income generation stopped, lost reputation or opportunity costs.

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 Fig 2

The nature of operational events is a function of its occurrence (frequency) and of its impact (severity). (Hoffman, 2002, Jordan, 2003)

(a) Recurring events: High frequency and low impact type. It is the best known part of operational risk, such as fraud in reporting claims. (b) 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 building 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 system and the culture of each organization. In this sense, the main difficulty in the management of operational risk is in the unavailability of internal database with which to approximate the variable used in the model. Therefore, solvency II rules allow, as does Basel II, to complete this data with the use of external database 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.

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 result 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 consisted of representatives of several international accounting and auditing organisations, and the report was undertaken by Coopers & Lybrand.

Internal control is defined as the process carried out by a company in order to assess, with reasonable assurance, the activities into three main categories. (KPMG, 2002) Effectiveness and operational efficiency, reliability of financial reporting, and compliance with policies, laws and regulations. This definition completes some fundamental concept 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 organization and procedural manuals; internal control only provide a reasonable degree of security, not the total 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: (a) Environmental of control (b) Risk assessment (c) Control activities (policies and procedures) (d) Information and communication (e) Supervision

On the other hand, Marshall, (2000) was of the opinion that 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 unit within an organisation, 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 according to King, (2001) needs an organisation 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, and skills of the company or management style). Together, these factors determine the way in which an organisation 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 other could affect 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 problem that risk raises,

supporting decisions in the scope of strategic management and in the sustainability of the competitive advantage. (Cristina, et.al 2008).

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 aspect. 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 strategic for growth of 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.

INSURANCE BUSINESS CYCLE AND RISKS

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 Fig 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 premium there is investment risk, and at all stage 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 values rather than the subsequent deviation of those expected values. Moreover, they do not cover all the risks to which insurers are exposed. Recently, due to advances in information systems and telecommunication, these models have become richer and more complex, incorporating all risks into one, and whose objective is the efficient allocation of capital.

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. In addition, the internal models propose a definition and measurement of capital requirement according to the characteristics of the activity of the company. However, these models produce a number of difficulties for 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 in 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 risk – based approaches that encourage a proper economic assessment and risk management from insurance and reinsurance companies.

With regard to solvency capital requirement, 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 mitigation and diversification of the company. To enable all companies 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 descend 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. (Gallati, 2003)

Models for Operational Risk Analysis of Insurance Companies VaR

From the study of model used in financial literature for the financial analysis of operational risks, 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. Of these, highlight VaR, extreme value theory and stress testing and scenario analysis models, Bayesian network 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 (Op VaR) 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. (Hussain, 2000)

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

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 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.

CONCLUSION

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 of other entities or individuals. Hence the strategic importance for citizens and governments that they protect their assets and income and their own 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 implication 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 modelling 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

- [1] Adeleye, B and F. Annansingh & Nunes, M (2004) Risk management practices in IS outsourcing: an investigation into commercial banks in Nigeria. *Inter. Journal of Information Management* 24(2), 167-180
- [2] Alexander, C. (2003), "Operational risk: regulation, analysis and management", London, Prentice Hall.
- [3] Bellando, J (2001), 'Assessing the financial health of insurance undertakings to protect the insured from the risks to which these firms are exposed: Solvency rules". Paris, OECD,
- [4] Basel Committee on Banking Supervision (2005), "Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework",
- [5] Chorafas, D (2004), "Operational risk control business opportunity and challenges for the insurance industry", Geneva Papers on Risk and Insurance: Issues and practice,
- [6] Committee on Banking Supervision (2001),"Operational Risk, Consultative Document: Supporting Document to the New Basel Capital Accord", Basel Committee on Banking Supervision.
- [7] Committee on Banking Supervision (1998),"Operational Risk Management, "Basel Committee on Banking Supervision.
- [8] Commission of the European Communities (2008), "Amended proposal for a Directive of the European Parliament and of the Council on the taking –up and pursuit of the business of insurance and Reinsurance (Solvency II) “, Commission of the European Communities, Brussels.
- [9] Coopers & Lybrand (2004), "Enterprise risk management –integrated framework: executive summary framework. “, Jersey. COSO
- [10]Cristina, B. O. Cornelia& Nicoleta, R. (2008) The necessity of Operational risk management and quantification. *Annals of Faculty of Economics* 3(1) 661-667
- [11]Di Renzo, B. M, Hillairet, & C, Bernard. (2007) Operation risk management in financial institutions: Process assessment in concordance with Basel 11 Software Process: improvement and Practice 12 (4), 3107-3127
- [12]Gallati, R. (2003), "Risk management and capital adequacy", New York, McGraw –Hill,
- [13]Hoffman, D. G. (2002), "Managing operational risk", New York, John Wiley & Sons,
- [14]Hussain, A (2000), "Managing operational Risk in Financial Market “, Butterworth Heinemann, Oxford.
- [15]Jordan, J, (2003): "Using loss data to quantify operational risk", Working paper, Bank of Boston.
- [16]KPMG (2002) Study into the methodologies to assess the overall financial position of an insurance undertaking from the perspective of prudential supervision, European Commission, Brussels.

