ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

Operational Risk Management in insurance through the process of Self Risk Assessment : Methodology of application

El Arif Fatima Zahra[1], Hinti Said[2]

1. PhD student – Department of Economics and Management, Center of Doctoral Studies, Faculty of Economic Sciences, University Mohammed V-Souissi, Rabat, Morocco.

2. Professor Authority – Department of Economics and Management, Faculty of Economic Sciences, University Mohammed V-Souissi, Rabat, Morocco.

Manuscript Info

Manuscript History:

Received: 10 October 2013
Final Accepted: 22 October 2013
Published Online: November 2013

Key words:
Operational risk, Solvency II, Self Risk Assessment, Risk Mapping

Abstract

The new European standard Solvency II has been applied since 2012 and replaced Solvency I. It imposed to insurance companies a new stringent regulatory framework, but more adapted to their appropriate risks. One of the big novelties is that the companies have the obligation to mobilize a part of their stockholders' equity on the cover from their exhibition to the operational risks.

Indeed, in its second pillar, the standard Solvency II, encourages companies to adopt the ERM (Enterprise Risk Management) approach, so that they are able by itself to estimate and measure their risks, in particular through the application of the device "Own Risk and Solvency Assessment (" ORSA ").

The objective of this paper is to present a methodological example of application of the approach of Self Risk Assessment (SRA) and mapping work in the context of operational risk management in insurance.

.

INTRODUCTION

Operational risk can be defined as the risk of loss resulting from inadequate or failed internal processes, human error, failure of computer systems, and external events.

So these are risks that have always existed in the insurance companies. It may be, for example, computer problems that slow down for a few hours employees that are ordinary and common problems, but it can also act as the local fire, as fire of Crédit Lyonnais, which had led to heavy losses.

Another more serious case is that of Société Générale in 2008, which recorded huge losses resulting from fraudulent positions taken by one of these traders Mr. Jérôme Kerviel. It would have exposed the bank to market risk as it was not within its remit: it would have accumulated long positions in futures contracts on index and conceals the transactions made on the market by introducing into the computer system of Société Générale fictitious offsetting the inverse operations. The causes of these important losses are internal fraud and failure in controls.

Operational risk is thus a risk that can be very expensive. For a long time, the regulations do not provide for its consideration. Today, this is done with the new Solvency II regulations.

In this article, we will outline the process of operational risk management in the context of modeling: the Self Risk Assessment (SRA) and mapping work, with their quantitative and qualitative objectives.

I. GENERAL OVERVIEW OF THE APPROACH

As part of a process of mapping, it is possible to distinguish among the many possible methods two main approaches. The first, is to use the process to identify the various risks of the insurance company, the second is based on a census of risks by the Executive Committee. These two possibilities are not opposed but complementary:

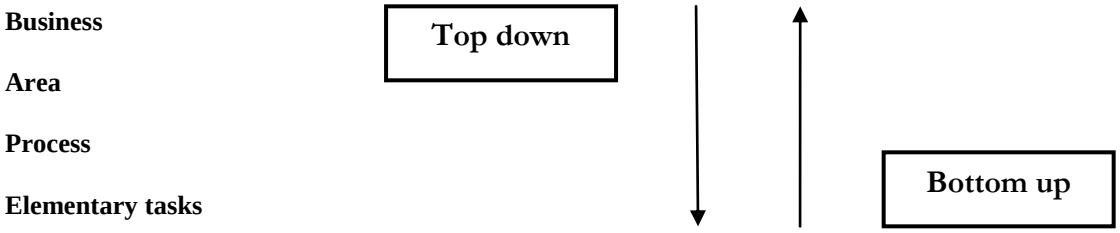

Figure 1. Complementarity of the two approaches

1) Approach "Top down"

This approach is based on an overview of the risk managers and to analyze these risks by experts.
The analysis of each of these risks by causes, control devices and associated consequences allows to estimate the parameters of risk quantification and conduct an assessment of each risk. This approach is called Self Risk Assessment. It has been deployed in workshops with internal business experts appointed by the Management Committees.
This so-called "top-down" approach provides at first a visibility on the main risks to which the Company is exposed. It is also an important vehicle information and awareness of the issues of operational risk.

2) Approach "Bottom-up"

The approach by risk mapping called "bottom-up" consists in analyzing in a comprehensive and systematic way, the operational risks and controls associated to every identified process. This is an important tool for guiding the operational risk for management, internal auditors and operational themselves.
This approach is based on two elements:
- Find an appropriate level of granularity. Too fine mesh involve too heavy construction and mapping that would result would be unmanageable daily. On the contrary, a too large mesh does not allow the control of operational risk. We have selected a level of granularity that will be explained later.
- Make sure of the implication of stakeholders of the operational management in the development of mapping. The owners of the processes and controls, internal auditors, managers and risk managers should be involved in the construction at first time, then in the updating of the tool in a second time.

3) Establishment of an incident basis:

Along with the mapping, it is essential to establish a base storied events occurred and operational risks associated with data loss. The creation of the database will:
- Corroborate or not the ratings for the first two approaches (based on a Self Assessment) and participate in the management of operational risks,
- To monitor risks and the effectiveness of controls in place,
- Feed the internal model for the calculation of economic capital.

II. PRINCIPLE OF SELF RISK ASSESSMENT

The major risks selected by the Committee are treated as follows:
For each risk, an analysis of scenarios must be made according to three assumptions: low, medium and high. This analysis is both qualitative (Causes / Effects / Control device), and quantitative (Frequency / Severity).
More specifically, the methodology of Self Risk Assessment of operational risks is divided into four steps:

Step 1: Scoping risk analysis

The expert defines and describes precisely the risk. This allows to define the scope of analysis. He accepts all potential situations of risk occurring.

Of all the identified risk events, he selects the one that seems most significant.

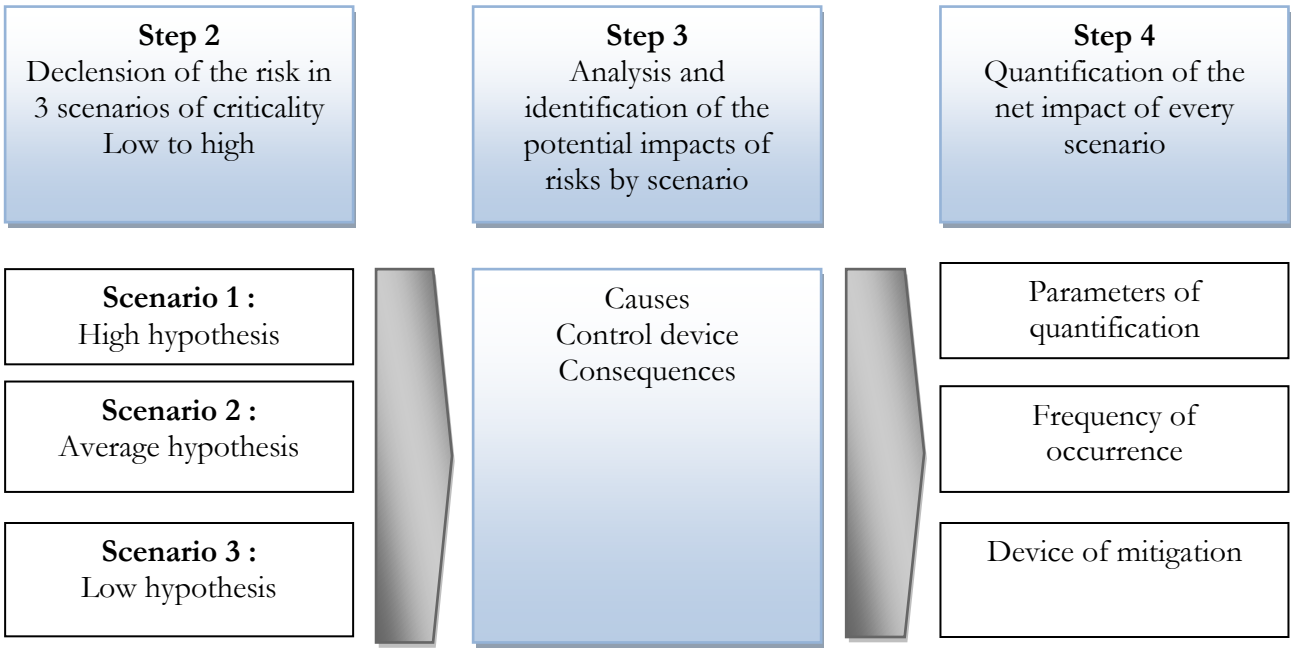

Figure 2. Scenario and Steps of Self Risk Assessment

Step 2: Determination of the context and the hypotheses of evaluation

The expert then makes hypotheses of analysis that each correspond to a scenario of gravity and increasing rarity: the low hypothesis is the lowest in terms of impact and frequency, and the high hypothesis is a severe condition. These hypothesis should be described precisely to allow qualitative and quantitative analysis of risk.

Step 3: Identification of the factors of qualitative analysis

Qualitative risk analysis based on the identification and description of the following factors : cause of the risk, control device, consequences.

- **The cause of the risk,** establishes the direct generative element of the event of analyzed risk.
- **The control device,** means all controls, procedures, systems, both internal and external monitoring indicators available to the insurance company to reduce the occurrence of the risk event and limit the impact in case of occurrence.
- **The consequences** is a subsequent effect on the occurrence of a risk event. It can be financial or qualitative. It can be direct or indirect: it is considered to be indirect when losses are consecutive to corrective actions taken by the entity.

To help the expert in his thinking, the risk manager presents him typologies of causes and consequences.

Once all the risk factors identified, it is to build combinations "Causes / Effects / device control" Associated with every hypothesis defined to allow the quantification of the impacts and the frequency.

Step 4: Identify the parameters of quantitative analysis

The quantitative analysis approach is to assess the consequences identified for each of the hypothesis previously defined, and the frequency of occurrence associated.
The qualitative effects are listed for information and may be subject to quantify as they give rise to indirect costs.
For each quantitative result, the expert must determine a precise formula for calculating the impact.
The sum of all these quantifications by hypothesis, give the overall financial impact of each scenario.
It is important to take into account for each hypothesis, the various mitigation and recovery to determine the net impact.
Determining the frequency of occurrence of each scenario is left to the appreciation of experts, based on their knowledge of the business and their own risk sensitivity, without any assistance in their decision is proposed to them.

III. EXAMPLE OF QUANTIFICATION OF RISK IN THE SELF- RISK ASSESSMENT

We present here a summary of technical specifications for the risk of error in the transition from order :

	Risk of error on the sense, the quantity or the code value in the seizure of an order		
	Low hypothesis	**Average hypothesis**	**High hypothesis**
	1 % of gap with regard to the market Less than 1% of the average NAV of the portfolio. Time error detection and NAV and de facto a risk of compensation) : a few hours. Amount of medium range order. Low in portfolio (5 M€)	2 % of gap with regard to the market Between 1% and 2% of the average NAV of the portfolio. Time error detection and NAV and de facto a risk of compensation) : one day Amount of medium range order. Medium in portfolio (50 M€)	5 % of gap with regard to the market Beyond 2% of the average NAV of the portfolio. Time error detection and NAV and de facto a risk of compensation) : several months Amount of medium range order. High in portfolio (250 M€)
Frequency	12 times every year	6 times every year	1 time every year
Financial consequences (K€)	175	825	15.500
Loss technical margin raw			
Direct financial loss Cost of communication / training Cost of rectification of the error Complaint customers Statutory penalties	175	825	15.500
Qualitative consequences			
Satisfaction customers / partner Assignment			
Statutory Incidence on the continuity Health and Safety Social climate Image reputation Consumer			High High

NAV = Net Asset Value

Figure 3. Our fact sheet for the risk of error

IV. APPROACH OF CONSTRUCTION OF A RISK MAPPING

The requirement for monitoring and control of risks, passes by the inevitable stage of operational risk mapping.
This step is all the more important for the insurance company, as it conditions the actions of reducation of the incidental risks and the system of reporting, as it contributes to the sizing of the control.
In a general way, the mapping consists in describing all processes and connecting it risks in particular to allow the internal control to target its actions and to prepare action plans.
The mapping requires beforehand the census of all existing processes listed in a process repository, and that of all the risks which can affect an insurance company, listed in a repository risks.

Level 1	Level 2	Level 3	Level 4	Level 5
Process Business	Manage Networks	Administer networks agents, brokers, providers	Agents	Select a provider

Table 1. Levels of risk mapping

Once this work was done, the mapping consists in identifying for each process the operational risks that could cause a loss in the process and how to quantify the average impacts of these risks.
Processes are then broken by level as risk. The process repository is divided into five levels of granularity:
_ Level 1 : Business (property and casualty, life, etc.).
_ Level 2 : Area (housing, car, etc.).
_ Level 3 : Processes (underwriting, sinister, etc.).
_ Level 4 : Operation (registration, regulation, etc.).
_ Level 5 : Elementary task (sending the check, etc.).

But for what level of process the mapping should be done?
The median level "process" seems to be the appropriate level of the mapping. It is on the one hand the best compromise between the time spent in the elaboration of the mapping and the degree of relevance of the vision of the risks. On the other hand, the equilibrium level for converging and connecting elements obtained from each of the two main methods (top-down and bottom-up).
It also seems that this level is relevant in the construction and the follow-up of a base incidental.

In the calculation of capital requirements, the mapping occurs especially to highlight the risks to be modeled. For this, experts determine the average frequency and the average severity of each risk, which will then be used to classify the risks in the matrix of Prouty.

Here is a theoretical representation of the matrix of Prouty, that crosses average frequency, and average severity of each risk:

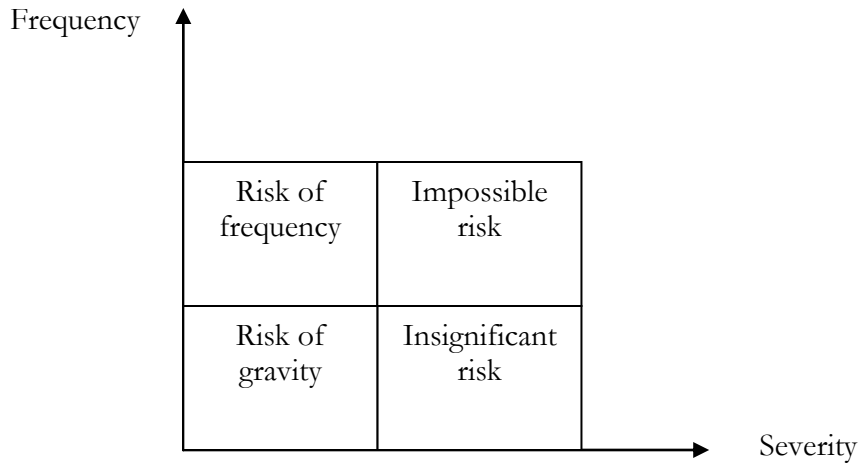

Figure 4. Matrix of Prouty

It follows four main categories of risk of this matrix:
_ **Insignificant risk** : low frequency, low severity. This type of risk is negligible;
_ **Risk of Frequency** : high frequency and low severity. The sinister has hit a low unit but often occurs. Its reduction is primarily the prevention;
_ **Risk of Severity** : low frequency and high severity. The loss is a rare but important or very important cost. Its reduction is primarily the protection and sometimes business continuity plan;
_ **Impossible risk** : high frequency and high severity. It must to be outside of the realm of possibilities to prevent the rapid disappearance of the company.
This classification will allow experts to identify the risks of frequency and gravity and to model them independently.

V. RISK ASSESSMENT METHODOLOGY

The question therefore arises is to know how to appreciate the risk: by frequency levels (very likely, likely, unlikely or very unlikely) or according to a financial appreciation of gravity (what is the cost estimated of the occurrence of a risk ?). The evaluation of a risk consists in bringing defensible information on the frequency and impact of the risk. The appreciation should be qualitative before being quantitative. However, this appreciation is generally insufficient and must be complemented by an assessment of the impact and frequency of occurrence. Indeed, **the raw risk** can be summarized by the following equation:

Raw risk = predictable impact x frequency of occurrence

The raw risk is rarely that actually supported by the company, because it would require a completely passive attitude of the latter.
It is indeed its impact before intervention of the elements of protection, the elements which lead to master totally or partially the risk to contain it in acceptable areas in terms of consequences. These control elements thus transform the raw risk into a residual risk.
It turns out, so commonly accepted that the assessment of raw and residual risks is the responsibility of the operational, which more easily apprehend impacts. However, this estimation has to be a confrontation with one or several persons in charge of the mapping to "validate" the hypotheses in terms of impact and frequency.
If necessary in case of difference of opinion, it may be helpful to resolve the issue by an ad-hoc committee.
Indeed, we may be faced with the fact that some operational tend to underestimate the potential impact of a risk for which they are responsible. Furthermore, it is possible that the operational do not think of the major risks with very low frequency. In any case, the entity in charge of developing the risk mapping has to watch the coherence of set, in particular to allow a relevant consolidation of risks.
To appreciate the elements of frequency is also a challenge for the development of the mapping. To achieve this, it is necessary to identify all possible sources of information (discussions with operational, internal auditors and external auditors, reading of existing audit reports, sector documents, internal bases incidents, etc.)..
The idea is to feed the argumentation to confirm the assessment performed. This then serves as a basis for discussion with the operational to get his opinion on this frequency.
Otherwise, it should proceed to arbitration in order to agree on a potential frequency.
This iterative approach then allows you to associate a frequency with every couple process / risk.
It is recommended to use a scale of frequency from 1 to 4, at least to most frequent, and of two levels of appreciation of this frequency: at time (the event occurs every day, all weekly, monthly, quarterly, 1, 5, 7, 20 or 100 years) and / or in volume (the event occurs in 1% of cases, 10% of cases, 0.1% cases, etc.).
The following table crosses these various elements:

Level	**1**	**2**	**3**	**4**
	Very unlikely	Unlikely	Likely	Very likely
In time	> 3 years	1-3 years	6 months -1 year	< 6 months
In volume	< 1%	1-5%	5-10 %	>= 10%

Table 2. Frequency range of risks in time and volume

The time scale can of course be adapted according to the strategy of the insurance, and the nature of the risks which it incurs.

By convention, it's better **to remember that the more the risk is big**, **the greater the number should be.** In addition, the proposed scale is a pair scale, in order to "take sides" and categorize the risk, what avoids the « average » risks, not allowing a meaningful analysis.

These evaluations are done in two phases:
• Risk taken into account assuming the passive company : raw risk;
• Risk taken into account with the measures already in place : residual risk.

The table below illustrates the evaluation process according to the possibilities of actual measurement of risk.

Estimation of :	**Qualitative**	**Semi quantitative**	**Quantitative**
The potential frequency of occurrence of the risk (f)		Null / Low / medium / high Or digital scale with an even number of levels	Average expected from the nb of emergence in the horizon of time chosen (Basel II: f=**Nxp**)
The potential impact in terms of financial cost (« severity »)			Amount on scale of continuous value (ex: million of €)
The potential impact in terms of image, challenged leaders	Description of the effets including: possible challenged of leaders	Scale of gravity according to objective criteria, with an even number of levels	To define on a case by case if possible (penalty: see supra financial impact.)

Table 3. Evaluation process according to the possibilities of effective risk measurement

* - **N**: Expectation for the time horizon (1 year), of number of generative events of the risk.
- **p**: Probability that the risk will occur during an event.
- In many cases, one of these two characteristics, in particular P, are not estimable, and / or it is easier to make a direct estimation of the annual frequency.

Examples of process of subscription of car contract

We focused on the analysis of this process to confirm the validity of the defined methodological tools. This process offers a double advantage, that to be shared by the largest number of insurance represented in the working group companies, and to be easily apprehensible by the not-specialists, the latter having for most cars to be personally insured.
The approach is performed in two stages, the first one consisting in validating the levels of granularity, and the typology of the risks.

We so held a structuring of the process as follows, according to the following list:
- **Process** : Level 3
- **Operation** : Level 4,
- **Elementary Task** : Level 5.

The process "Car Subscription" can be then cut in following elements (number in parenthesis corresponds to the level of granularity):

1. Selling Car Contract (3)
   - Collection of informations (4)
     Statement of information (5)
   - Issue estimate (4)

2. Subscription (3)
   - Acceptance (4)
   - Recording (4)
   - Issue of police (4)

3. Cashing premium (3)
   - Issuance of receipt (4)
   - Recording (4)
   - Cashing (4)

Discount of the check (5)
Transfer (5)

The relevance of the typology was appreciated through the process of development of a product offering in car insurance.

CONCLUSION

In a more and more complex and unpredictable world, the Leaders of insurance companies understood well that the risk management guaranteed economic information, strategic, structural or operational, more reliable and of better quality.

Even if the persons in charge of insurance companies have a vision and a global approach of the inherent risks to their activities, build a risks mapping can only bring them new elements of observation intended to master better and to direct their objectives.

This is why the leaders must be convinced of a value of risk mapping, encourage and participate actively in its implementation.

The applications of a risk mapping are numerous and lead the users to prefer such or such aspect of the results obtained to redefine their priorities.

Of the Board of directors to the Head office, by way of the operational managers, risk managers, internal controllers and internal auditors, everyone can use the mapping as a support for their own organization actions.

Any risk mapping should not be an end in itself, but a starting point for action. Simple in its principle but complex to develop, a mapping must first have the approval and support of all participants, so that the results reflect the reality of the organization and its risks.

During and after its completion, operational have to appropriate the mapping by becoming aware of important and essential risks, take a proactive approach to analyze these risks, finally, define an action plan to reduce exposure to identified risks.

The success of a risk mapping lies in its future use, in the ability of users to make it live in time.

References

1. Alexander, C. (2003) : *Operational Risk: Regulation, Analysis and Management*, FT Prentice Hall, London.

2. Basel Committee on Banking Supervision (2001) : *Working Paper on the Regulatory Treatment of Operational Risk*.

3. Baud N, A, Frachot, T, Roncalli (2008), An Internal Model for Operational Risk Computation.

4. Boyer, M., G. Dionne et C. Vanasse (1991) : "Econometric Models of Accident Distributions", in G. Dionne (ed.): *Contributions to Insurance Economics*, Norwell, MA: Kluwer Academic Publishers.

5. Chernobai, A., C. Menn, S. T. Rachev et C. Trûck (2005c) : "Estimation of Operational Value-at-Risk in the Presence of Minimum Collection Thresholds." Technical Report, University of California Santa Barbara.

6. Dahen H (2006) : La quantification du risque opérationnel des institutions bancaires, thèse.

7. Dionne, G. et C. Vanasse (1992) : "Automobile Insurance Ratemaking in the Presence of Asymmetrical Information", *Journal of Applied Econometrics* 7, 2, 149-165.

8. Hartung, T. (2004) : "Operational Risks: Modelling and Quantifying the Impact of Insurance Solutions", Working Paper, Institute of Risk Management and Insurance Industry, Ludwig-Maximilians-University Munich, Germany.

9. Hugues C., Tristan P. (Octobre 2006) : Le contrôle interne, Objectif confiance, La Tribune de l'Assurance n°105

10. Jobst A. (Avril 2004) : Consistent Quantitative Operational Risk Measurement and Regulation: Challenges of Model Specification, Data Collection, and Loss Reporting.

11. Na, H. S., J. Van Den Berg, L. C. Miranda et M. Leipoldt (2006) : "An Economic Model to Scale Operational Losses", *The journal of Operational Risk* 1, 2, 11-31.

12. Scandizzo, S. (2006) : "Scenario Analysis in Operational Risk Management", ", *The Advanced Measurement Approach to Operational Risk*, edited by E. Davis, Risk Books, London.

13. Tripp M H, H L, Bradley, R, Devitt, G C, Orros, G L, Overton, L M, Pryor, R A, Shaw (Mars 2004) : Quantifying Operational Risk in general Insurance Companies.