Chapter 17.

THE IMPORTANCE OF OPERATIONAL RISK MANAGEMENT IN INSURANCE INDUSTRY[1]

In previous years we have witnessed the globalization of the financial structure of the international economy. Mentioned process has led to the appearance of serious risks of the insurance companies and the world's economy as well. In order to stable development of its business and equal participation in a large competitive market, primarily for the protection of its customers and preserving the system stability and liquidity, insurance companies have to build in their strategic goals into risk management strategies. Until recently, attention was mainly focused on the security risks and the risks of investing.

However, more complex operational functioning of insurance companies has led to a greater sensitivity to other risks that could jeopardize the business of insurance companies, one such risk is operational risk. Operational risk is one of the most difficult business risks for both the insurance company and for its customers. Operational risk management is not a new concept for financial institutions. The stability of information systems, customer requirements, or errors in internal control was followed for years. Yet, all of these elements are previously treated separately. Turning point in the consolidation and standardization of operational risk has brought Solvency II.

Bearing in mind the fact that operational risk arises from imperfection of business processes and technology systems, it is difficult, and in many cases impossible to do prediction based on historical data, it is necessary to pay special attention on this topic.

The aim of this chapter is to explain the concept of operational risk, and operational risk management processes with regard to the framework provided by Solvency II.

[1] The authors gratefully acknowledge the financial support of the Ministry of Education, Science and Technology of the Republic of Serbia, Grant No. 179015 and 47009.

1. CONCEPT AND TYPES OF OPERATIONAL RISK

Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, human errors, system errors or external events.[2] The basic components of operational risk include: errors in information systems, failures in the control of financial reporting, planning and implementation of projects; inadequate organizational structure. The operational risks in the wider sense include: the risk of human resources (human capital risk), risk management (management control risk), the risk of a computer system (system risks), strategic risk (strategic risks), the risk of procedures (process risks), legal risk, the risk of loss of reputation (reputation risk), the risk of realization of a catastrophic event (disaster risk), a regulatory risk (regulatory risk), political risk (political risk). [3]

Operational risk arises from the following situation:
1) growing use of automated technologies that can lead to system errors, given the increasing reliance on information technology and systems;
2) the growth of e-business, leading to a potential risk that is still not fully understood (eg, internal and external theft and security issues of the system);
3) mergers and acquisitions, ie. creating a major business entity that is difficult to manage;
4) use of sophisticated product for the management of financial risk.[4]

This type of risk is related to the situation when a loss may occur as a result of incorrect handling the transaction and information processing, also as a result of fraud and system failure. It should be noted that the operational risk becomes evident because of the increasing use of information technology and automation in the financial business, introduction of complex securities, etc. In general, it can be concluded that operational risk is the result of improper functioning of the system.

[2] Russell-Jones, N., Alastair, D. (2004). Risk analysis and evaluation. Edinburgh: The Chartered Institute of Bankers, p. 100.

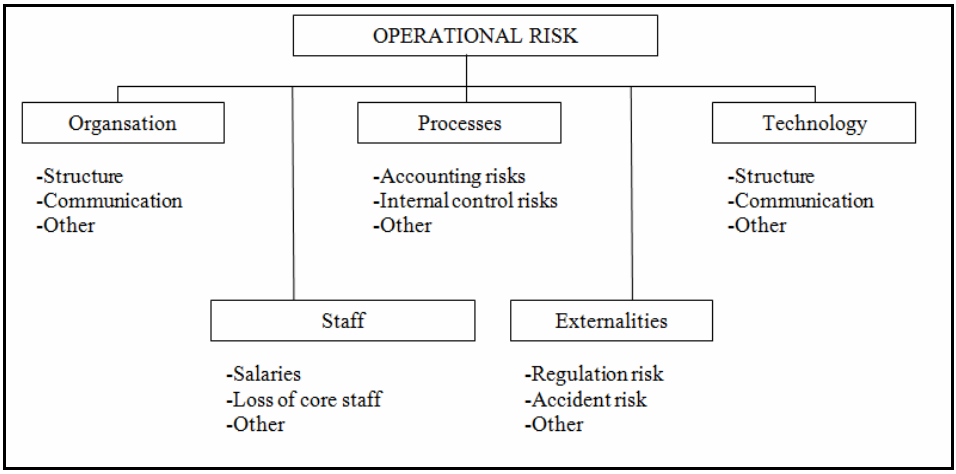
[3] Komelj, J, Dolničar, J. (2007). *Izazovi i mogućnosti u osiguranju i reosiguranju s naglaskom na Solventnost II.* Ljubljana: Pozavarovalnica Sava d.d., 16. June 2007, p. 7.

[4] Bank For International Settlements (2003). *Sound Practices for the Management and Supervision of Operational Risk.* Basel: BIS, p. 1

There is a tendency in recent years to find the basic concept of operational risk. Almost all definitions emphasize the inner side of the operation, but there are often unexpected external events also classified as operational risk. Many approaches speak about of loss and the direct financial losses, and also the indirect must be considered - those which are published by the loss of reputation and loss of its market position. It is considered to be one of the best definitions of operational risk the one that is given by The British Bankers' Association: "*Operational risk is the risk of direct or indirect loss resulting from inadequate or failed internal processes, personnel and systems, or due to external events.*" When this definition is adapted general definition of risk gives the following definition: "*Operational risk is a term dangers of direct or indirect loss resulting from the inadequacy of internal processes, people and systems or due to external events.*". Generaly researchers aproaches has few common characteristics about operational risk: they are focused on the quantification of operational risk and they are based on the definition of operational risk as prescribed by Basel II.[5] *Caudhury (2010*) wrote on developing the capital adequacy models of operational risk for banks. Until now only few papers i.e., Verrall (*2007*) and Tripp *et al* (2004) focused specifically on the operational risk of insurance companies and Cummins et al (2006) focused on both banking and insurance in their publications. In line with the Basel II requirements, Scandizzo (2005) provided a systematic method for mapping operational risk in the process of its management. Operational risk is categorised into internal and external sources by some authors e.g., Cummins *et al*., (2006); Dickinson, (2001); Guillen *et al*., (2007). A number of studies: Jobst (2007), Moosa (2008) and Flores *et al*. (2006) have discussed several statistical techniques for operational risk measurement and subsequent regulatory requirements.

[5] Acharyya, M. (2012). Why the current practice of operational risk management in insurance is fundamentally flawed - evidence from the field. *ERM Symposium,* April 18-20, 2012.

Figure 1. Definition of operational risk



The above set of different risks is known as operational risk. This is the risk of loss, as already stated, due to improper or failed internal processes, people or systems or due to external influences. The definition includes legal risk, but includes strategic and reputational risk also.

2. SOURCES OF OPERATIONAL RISK

A specific approach to operational risk management chosen by particular insurance companies depend on a number of facts, including its size and the level of technical equipment, as well as the nature and the complexity of its activity. However, regardless of these strategies, a clear strategy and control the board of directors and senior management, strong culture of operational risk, as well as the culture of internal control (which, among other things, include a clear hierarchy of authority and segregation of duties), effective internal reporting and planning in the event of unforeseen circumstances, are the key elements of the framework for an effective operational risk management of insurance company.

Deregulation and globalization of financial services, coupled with rising levels of financial technology, make the activities of insurance companies increasingly complex.[6] As an example of these new and growing risks are set out as follows:

- If not properly controlled, the increased use of highly automated technology can turn risks arising from errors in manual data processing system at risk, due to the increased presence of relying on global integrated system;
- the growth of e-business brings with it potential risks (eg, internal and external fraud and questions sigrnosti system), which are not fully understood;
- Acquisition, merger, division and consolidation of large-scale testing of new or daring recently integrated systems.
- Regardless of the exact definition, the effective management of risk and control of this risk category, it is essential that insurance companies clearly understand what is meant by operational risk.

It is also important that the definition takes into account the entire set of significant operational risks faced, and thus to include the most important causes of serious business losses. Insurance companies are required to identify existing sources of operational risk, as well as potential sources of the risks that may arise from the introduction of new products, systems and activities. Identifying sources of risk implies:[7]

1. Internal errors and abuses :
   - Unauthorized actions of employees,
   - Abuse of authority.

2. External violations including:
   - Unlawful conduct of persons who are not employed by the insurance company,
   - Gaps in the security system;
   - Gaps in the system of employment and safety at work:
   - The relationship between employees of an insurance company,
   - Safety at work,
   - Discrimination in the workplace.

[6] Wei, R. (2003). *Operational Risks in the Insurance Industry.* The Wharton School, University of Pennsylvania, p. 2.

[7] Epetimehin, F.M. (2013). Managing The Impact Of Operational Risk On The Solvency Of Insurance Companies, *OIDA International Journal of Sustainable Development*, 5(2), pp. 69-78.

3. Problems in the functioning of relationships with customers, product marketing and business procedures - if they are inadequate:
   - Standardization of products, the protection of information and trade secrets,
   - Operational procedures,
   - Business flows (flows -making and information flows)
   - Choice of clients and exposure to them,
   - Advisory function;
   - Damage to property insurance company due to natural catastrophes and other events;
   - Disturbances in the organization of the insurance company and the errors in the functioning of the established systems.

4. Implementation of business processes and decisions:
   - monitoring and reporting,
   - Receive clients and documentation
   - management of claims and obligations to clients,
   - relationships with other business partners,
   - Relations with suppliers.

Active exchange of ideas between supervisors and sector of insurance is essential for the continued development of appropriate guidelines for the management of exposures that are associated with operational risk.

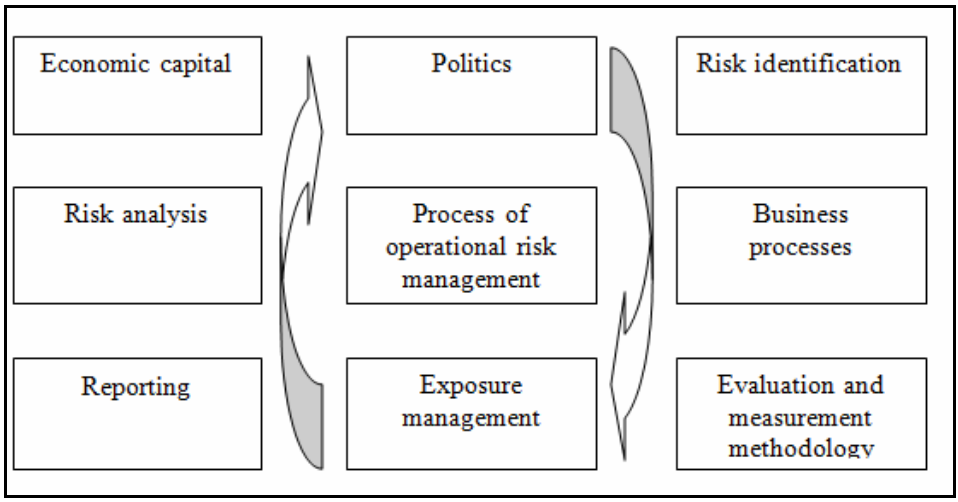
3. OPERATIONAL RISK MANAGEMENT

Risk management is a central part of strategic management and corporate governance of any organization. Operational risk management as an integral part of risk management is part of the strategy and operational decision making in insurance company. The evolution of the operational risk management as a management function is a regulatory driven approach which binds managers to must compute the level of risk capital.[8] The success of the implementation process of operational risk management basically depends on the availability of information and expertise of employees in the insurance company. Three groups

[8] Acharyya, M. (2012). Why the current practice of operational risk management in insurance is fundamentally flawed - evidence from the field. *ERM Symposium,* April 18-20, 2012, p. 5.

of professionals are interested with the management of operational risk in practice: internal auditors, risk modellers, business managers.

Figure 2. Managing operational risk



It can be argued that the main objectives of operational risk management are:
- Providing protection from potential events that manifest operational risk
- Mitigate the effects arising in the operational risk and reduce its impact, and
- Adequate control of any damage in the event of operational loss events.

It is important to emphasize that the structure of the process of operational risk management as an integral part of the process of risk management in the insurance company, it must be safe, effective and economical. Operational risk is due to its specificity present in each activity and its successful management involves precisely defined function for managing operational risk in terms of the roles and responsibilities of all stakeholders and adequate organizational structure in an insurance company. Basis for establishment of an efficient and reliable system of risk management is accurate and timely information on all the relevant data, and software support for the implementation of an adequate model for managing operational risk. In order to establish the operational risk management of the bank is required to develop a four-phase framework to manage this risk:

1. Identification:
   - Definition,
   - Determine the extent of the risk,
   - Classification (category under the - category, action);
2. Rating:
   - Self-evaluation,
   - Scoring risk
   - Risk mapping,
   - Risk measurement.
3. Control:
   - Policy
   - Management programs,
   - Guidance control
   - Management structure,
   - Reporting structures.
4. Monitoring:
   - Integrated internal and external controls,
   - Periodic evaluation,
   - Regular reporting.

A key strategy for managing operational risk can be directed to the identification of key processes and the types of operational risk arising from these processes, relating to people, communication products and systems. The first step in adopting the program of operational risk management is that employees of the insurance company to adopt a definition of operational risk. In other words, the identification phase is of utmost importance to participants in the process of operational risk management understand the risk event because, according to some estimates, about 30% of the data entered in the appropriate database of operational risk is wrong. Risk identification is the most important is maintained in the subsequent development of the monitoring and control of operational risk. Effective identification of operational risk takes into account both internal factors (such as the structure of the insurance company, the quality of human resources, organizational changes and turnover per employee) and external factors that can adversely affect the achievement of the objectives of the insurance company. Management identified operational risk involves a choice between four alternatives:

1. Risk-taking,
2. Risk avoidance,
3. Mitigation,
4. Sharing and risk transfer.

Identification of operational risk

In addition to identifying potential operational risks, insurance companies are required to assess and extent of their vulnerability to these risks. Effective evaluation of operational risk is a way for insurance company to a better understanding of the best way to direct its resources to manage the risk. Risk assessment determines the level of risk within the business units. As a possible tool for assessment of operational risks are discussed:

1. Self-assessment of risk;
2. Packaged (mapping) risk;
3. Indicators of risk (risk rating);
4. Risk measurement.

Self-assessment of operational risk

Self-assessment involves a process in which an insurance company assesses the operations and activities with respect to the catalog of sensitivity to operational risk. This process is carried out inside and often involves control processes or workshops to determine good and bad characteristics of the environment in which the present operational risk.

Self-assessment is the process in which business units:

- Identify and evaluate risk,
- Identify and assess the level of control that have been established for risk management,
- Prepare plans for improvement (operational risk management program).
- The necessity of self-assessment stems from the fact that it:
- Determine responsibility for operational risks within the business unit - business unit take responsibility for operational risks and losses arising from such risks;
- Reinforce a culture of openness and transparency - the determination of appropriate resources and increasing awareness of operational risk requirements openly talking about them;
- Implement a proactive rather than a reactive process - the business will be more successful if they adopt conclusions on business or in advance, i.e. Before problems arise;
- Identify gaps - identify the gaps in controls and prepare assignments to remedy these deficiencies;
- Enhances insight and decision-making - to better understanding of exposure risk management insurance companies carefully examine the results of self-assessment;

- Improve audit productivity - improve the reliability of self-assessment, the auditors the opportunity to commit the key issues faced by the insurance company faces.

Risk classification is the process in which the various business units, organizational functions, or business processes are classified according to the type of risk. Applying this task can detect areas of weakness, to provide assistance to management about setting priorities for further activities. Risk indicators are statistics and/or metric information, often financial, which may provide insight into the risk position of the insurance company. By measuring the risk, insurance companies are trying to determine the extent of its operational risk exposure using a variety of approaches. For example, data on the experience of the insurance company related to historical loss can serve as a good basis for the assessment of exposure to the insurance company's operational risks and develop policies to reduce this risk. One way to successful utilization of this information is to establish a system for the systematic monitoring and recording the severity and frequency of certain cases of loss , and other relevant information about them [9].

Control activities for operational risk

Control activities are designed in order to comply with the operational risk that the insurance company identified and assessed. With respect to each of the identified operational risks, the insurance company has to make a decision on whether to use the proper techniques for controlling and reducing the risk, or will otherwise bear the risk. When it comes to those risks that can not be controlled, in such circumstances, the bank or decide to accept the risk, reduce the level of business-related activities, or decides to withdraw completely from the activity. Operational risk control helps in its management and reporting. For this reason, the insurance company should introduce regular process of controlling operational risk profile and exposure to significant losses.

A successful process of control is critical to the proper management of operational risk because these activities may lead to timely detection and correction of deficiencies related to policies, processes and procedures for managing operational risk. Insurance companies should have policies, processes

[9] Acharyya, M. (2012). Why the current practice of operational risk management in insurance is fundamentally flawed - evidence from the field. *ERM Symposium,* April 18-20, 2012.

and procedures for monitoring operational risk. One must periodically review its strategy for ograničavanje and controlling risks to align its risk profile with the use of applied strategies. Processes of control operational risk, which are part of the regular activities of the insurance company, providing a timely response to changing condition and avoid unnecessary costs. A successful system of internal control includes a specific allocation of responsibilities and competencies so that staff are not distributed in a way that could result in a conflict of interest. However, in addition to segregation of duties, the insurance company should ensure the existence of other internal practices suitable for controlling operational risk.

Operational risk may be greater in cases where the insurance company move on to new activities when establishing new products, or acting in an unfamiliar market or start their own business in places that are far away from the seat of an insurance company. In such situations, many insurance companies do not provide the infrastructure management controls risk increases with increasing business. The biggest losses incurred as a result of the above activities. For this reason, particular importance is the requirement that insurance companies, when there are such circumstances, to ensure that the activities of internal and external control of special attention.

Monitoring of operational risk

Insurance companies should look at actions for reducing risk as supplements to basic internal control operational risk, and not as a replacement. Mechanisms for identifying and testing operational errors can contribute to a significant reduction of operational risk, where it is necessary to carefully consider the extent to which these mechanisms reduce risk (eg. Reinsurance) contribute to its real reduction, and the extent to which it is transferred to another sector , area businesses or even influence the creation of new risks (eg legal risk). Successful monitoring process is essential for the proper management of operational risk and should be an integral part of the activities of insurance companies. This process can explicitly provide assistance in determining the key significant risks and enable the insurance company to properly approaches to that risk.

Insurance companies are trying to introduce a process of regular monitoring of operational risk profiles and material exposures to losses. Mechanism for regular monitoring can contribute to faster detection and examination of deficiencies in policies, processes and procedures for managing operational risk, while rapidly eliminating these shortcomings and addressing them can

significantly reduce the incidence or severity of the potential loss. The frequency of monitoring should reflect the risks present, the frequency and nature of changes in the business environment. In addition to monitoring the occurrence of operating losses, the insurance company must determine which data will be fast enough to warn of the increased risk of future losses. Key risk indicators and early warning indicators should be directed to future operations, where they can reflect potential sources of operational rizka, for example. rapid growth, the introduction of new products, turnover per employee, etc. Results related activities of insurance companies should be included in the regular reports of government insurance companies. Also, the results of internalization of respect for the rules that implemented the function responsible for monitoring may include information about the track, where of him must be notified senior management and the board of the bank, if needed. Management may also make use of the reports prepared by external sources (auditors and supervisors) and analyze them to improve the performance of existing operational risk management. Mission of operational risk management would be to identify, analize and reduce various risk operations. New regulation of Solvency II will increase the need of an effective management of operational risks by development and implementation of complex methodologies for the analysis.

3. SOLVENCY II APPROACH TO OPERATIONAL RISK MEASUREMENT

One of the major expected contributions of the Solvency II concept, as a forthcoming regulatory framework for insurance companies operating in the European Union, is exactly the recognition of the importance of operational risk, which was historically neglected in the field of insurance and reinsurance. Considering the fact that operational risk is one of the crucial threats to the solvency of insurance companies, it is recognized as a separate risk category, along with insurance, market, credit and intangible assets risks. The insurers' solvency regulation, EU Solvency II in particular, adopted operational risk as one of the core risk of insurance business. Under Solvency II there are two possible approaches to modeling operational risk exposure: a standard or factor-based approach or the use of an internal model.

Proceeding from the assumption that the size of the insurer is strongly associated with the severity and number of its operational losses, solvency capital requirement for protection against operational risk is computed on the

basis of the amount of insurer's premiums and technical provisions. Also, with respect to life insurance contracts where the investment risk is borne by the policyholders, the calculation of the capital requirement for operational risk shall take into account the amount of annual expenses incurred in respect of those insurance obligations.[10] Since it is very difficult to unbundle the effects of operational risks in an insurance company from other types of risks, given risk is treated as perfectly correlated with other risk categories when aggregating the respective capital requirements within the standard approach.

According to the technical specifications of the last quantitative impact study (QIS5), the solvency capital requirement for operational risk (SCR_{Op}) is determined as follows:

$$SCR_{Op} = \min\left(0.3 \cdot BSCR; Op\right) + 0.25 \cdot Exp_{ul} \tag{1}$$

where

$BSCR$ - Basic Solvency Capital Requirement for six risk categories (i.e. market risk, counterparty default risk, life underwriting risk, non-life underwriting risk, health underwriting risk and intangible assets risk);
Exp_{Ul} - amount of annual expenses in previous year incurred in life insurance activities where the investment risk is borne by the policyholders;
Op - basic operational risk charge for all business other than life insurance, where the investment risk is borne by the policyholders, which is calculated according to the following:

$$Op = \max\left(Op_{premiums}; Op_{provisions}\right) \tag{2}$$

$$\begin{aligned} Op_{premiums} = {} & 0.04 \cdot \left(Earn_{life} - Earn_{life-ul}\right) + 0.03 \cdot Earn_{non-life} + \\ & \max\left(0; 0.04 \cdot \left(Earn_{life} - 1.1 \cdot pEarn_{life} - \left(Earn_{life-ul} - 1.1 \cdot pEarn_{life-ul}\right)\right)\right) + \\ & \max\left(0; 0.03 \cdot Earn_{non-life} - 1.1 \cdot pEarn_{non-life}\right) \end{aligned} \tag{3}$$

[10] EC (2009). 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). *Official Journal of the European Communities,* 2009/138/EC, article 107.

where $Earn_{non-life}$, $Earn_{life}$ and $Earn_{life-ul}$ represent earned premium during the previous year in non-life insurance, life insurance and life insurance where the investment risk is borne by the policyholder, respectively. Similarly, $pEarn_{life}$ and $pEarn_{life-ul}$ refer to earned premium during the year preceding the previous year, for life insurance without and with the transfer of investment risk to policyholders, respectively. Finally,

$$Op_{provisions} = 0.0045 \cdot \max\left(0; TP_{life} - TP_{life-ul}\right) + 0.03 \cdot \max\left(0; TP_{non-life}\right) \quad (4)$$

where, analogously to the previous, $TP_{non-life}$, TP_{life} and $TP_{life-ul}$ indicate technical provisions in non-life insurance, life insurance and life insurance where the investment risk is borne by the policyholder, respectively. For the purpose of the presented calculation, earned premium should include amount of premium ceded to reinsurance. Also, technical provisions should not include the risk margin, and should be without deduction of recoverables from reinsurance.[11]

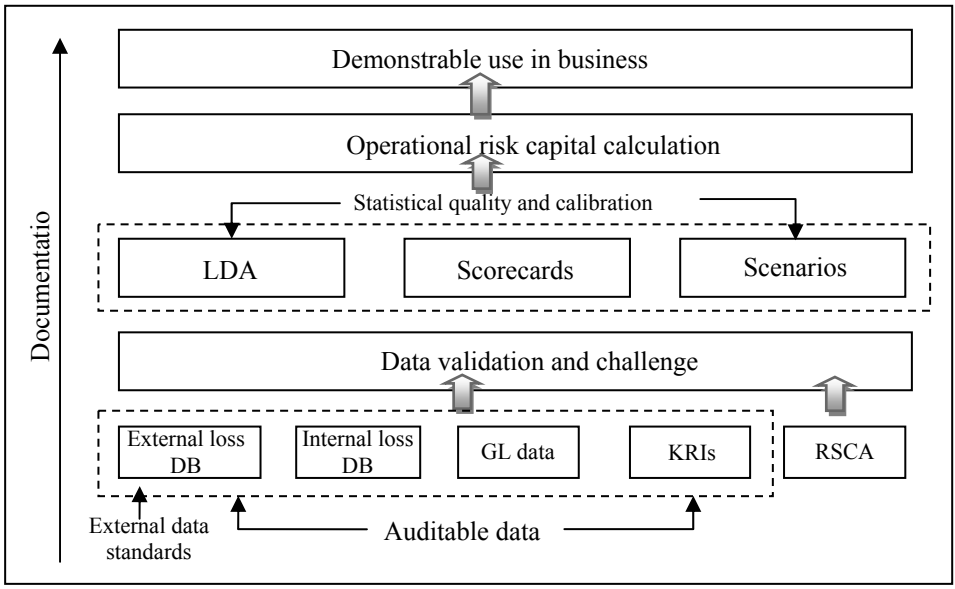
There are a number of objections that can be made to the standard formula for the calculation of capital requirements on the name of operational risk. Namely, due to its simplification, this formula is not risk sensitive and generates undesirable incentives for insurers to underestimate their own premiums and technical provisions in order to express relatively lower capital requirement. Since it does not take into account the quality of the operational risk management processes of particular insurer, the formula does not encourage the development of good risk management practices. Also, the formula does not reflect the wide spectrum of operational risks that can materialize within an undertaking.[12] Due to the extremely high complexity and heterogeneity of operational risk, it is very difficult to find a standard formula that reflects the operational risk that would be relevant across different insurers and jurisdictions. As operational risk has a wide range of qualitative aspects which

[11] EU Commission (2010). *QIS5 Technical Specifications.* Brussels: European Commission, p. 102.

[12] CEIOPS (2009). CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: SCR standard formula - Article 111 (f) - Operational Risk. *CEIOPS-DOC-45/09.* Frankfurt: Committee of European Insurance and Occupational Pensions Supervisors, p. 7.

cannot be taken into account reliably in the standard formula, there is a need for objective and precise treatment of operational risk within appropriate internal models. Internal-model approaches to operational risk include identification of a set of operational risk scenarios and derivation of a loss distribution for each of them, on the basis of expert judgment. Also, correlations between scenarios have to be assessed in order to aggregate scenario results and produce a capital charge.[13]

Figure 3. Example of an internal model option under Solvency II



Source: Ernst & Young (2008). Measuring operational risk. Solvency II Global Insurance Center. London: Ernst & Young Global Limited, p. 2.

In terms of lack of credible data and unfinished pillar II infrastructure, the simple standard formula is the logical refuge for most insurance companies for the determination of operational risk capital requirement, even for those large insurance groups that already have developed internal models for other risk categories. Also the banking industry's experience indicates that many

[13] Cantle, N., Clark, D., Kent, J., Verheugen, H. (2012). A brief overview of current approaches to operational risk under Solvency II. *Milliman White Paper,* London: Milliman, p. 2.

organizations are avoiding internal-model approaches primarily because of high development and implementation costs and the perceived small return on their investments.[14] It is obvious that, along with an increase in insurer`s focus on operational risk, Solvency II will produce a number of difficulties and challenges for their risk management activities. At first, insurers will need to develop appropriate documentation, improve the quality of their data and data-gathering techniques, which form the basis for measuring operational risk exposure and their successful management. The missing internal and external data can be compensated by the implementation of appropriate scenario analysis within Own Risk and Solvency Assessment (ORSA), as an integral element of the second pillar of Solvency II concept. However, existing methods of scenario analysis that insurers internally use are often too complex, inconsistently applied in space and time and therefore - inefficient and ineffective.[15] Therefore, the scope for further improvement of the treatment of operational risk within the concept of Solvency II should be sought on the side of techniques and tools that insurers use to support risk self-assessment, rather than on the side of too crude and arbitrary pillar I standard-formula for explicit calculation of operational risk capital charge.

Insurance companies face many risks. The complexity of these companies comes from the nature of their business, which is reflected in the risk-taking of other entities or individuals. Because of various operations and processes these organizations have on a growing implications and interactions with other risks this brings them face with such as market and credit risks. Consequently, the operational risk is increasingly important in management and corporate governance of insurance company. Internal operational losses can be caused by junior staff; but they can also be caused by mid-level officers, senior managers, C level executives and Boards of Directors. They are sometimes caused by individuals and in other cases by groups of people working in collusion. The largest losses often take place when operational failures are present at the senior-most level. This might include situations where senior executives are themselves engaged in inappropriate risk-taking or even outright fraud, or perhaps more commonly, where executives intentionally overlook such actions by junior staff because they themselves are benefiting in the form of short-term

[14] Ernst & Young (2008). Measuring operational risk. *Solvency II Global Insurance Centre.* London: Ernst & Young Global Limited, p. 2.

[15] Van Grinsven, J.H.M., Bloemkolk, R. (2009). Solvency II: Dealing with operational risk. *FSI Magazine,* #5 April, 2009, p. 4.

financial incentives.[16] It is the best to model operational risk by combining internal loss data, external loss data (data from other institutions) and expert opinion. Analysis of operational risk is a necessary activity for all stakeholders and represents a important opportunity for development and areas of expertise in the field of insurance, because the specificity and the complexity involved in this kind of risk.

Solvency II, as a new regulation is structured into three pillars: financial conditions in accordance with the actual level of risk assumed by the insured, the internal control mechanisms and transparency of the market and disciplines.

The insurance sector in Serbia is facing a strategically important task to develop a good framework for operational risk management. As an aggravating circumstance that can uspriti this process is that it is a risk that a poorly known domestic market which is still not given much attention, and for that reason need significant time to develop employees' awareness of the risks, and to raise the culture of behavior at all levels of the insurance company in relation to exposure to operational risk and its management at all levels.

[16] Society of Actuaries (2010). *A New Approach for Managing Operational Risk, Addressing the Issues Underlying the 2008 Global Financial Crisis*. Schaumburg: Society of Actuaries, p. 25.