Dejan Jednak[1], Jovo Jednak[2]
[1]Privredna banka Beograd a.d., Beograd
[2]Belgrade Business School, Belgrade

Operational Risk Management in Financial Institutions

The current economic crisis and a great number of individual examples indicates that the cumulative operational risks in the financial industry cause domino effects, which can lead financial institutions to the zone of extreme losses, or even to bankruptcy. Furthermore, operational risks are heterogeneous and very complex and can generate disproportionately high losses, since they interact with other risks (multiplying their effects). In the conditions of the global financial crisis, operational risk becomes a dominant risk. Additionally, the cumulative operational risks can act independently or supplementary as the cause of crisis in the financial system. This has been proved during the last couple of decades both in Serbia and in the broader area of the Central and Southeast Europe. The experience so far has confirmed that current statistical and mathematical methods for measuring VaR have not yielded the expected results, especially from the aspect of valid and precise risk assessment. Internal and external events that initiate operational risks are very specific and unpredictable. That is why VaR has to be adjusted, although it is a standard risk measure in the deposit financial institutions. Accordingly, the paper provides the alternative solutions for the projected risk models in order to calculate the events of low or middle value, i.e., to envisage the probabilities for the external events in order to absorb, or to efficiently manage the risks.

Keywords: Operational risk, financial crisis, loss, heterogeneousness, volatility, model risk, moral hazard

Introduction

Constant exposure of financial institutions to different sorts of risk, and the complexity of the methods for their identification, assessment, monitoring, control and measuring, i.e., the process of integrated risk management has reached the highest level of business-expert thinking and decision making. The financial industry has, above all, developed the standard methods for managing and measuring market and credit risks, but the operational risk as well. However, it turned out to be a very important cause of financial losses (Di Renzo et al, 2007). Since the majority of financial bankruptcies stem from joint effects of market, credit and operational risks, risk management should be an integral part of corporate decision making through business activities and types of risks. Financial institutions are being exposed to the intensified global sources of risk, due to the expansion of their own business activities, interaction between different risk factors and the connection between products and services with different types of market, financial and operational risks (Wu & Olson, 2010). Among other risk types that come with the activities of the financial sector, the economy and other types of organising business, operational risk holds a special position. Its very nature to be expressed in the fluid form and its presence in all segments of business activities tell enough of its importance and the need to manage it efficiently. Throughout the history, operational risks were managed by internal control mechanisms within business units, supported by audit. Nowadays, the financial industry has begun to use special structures and control processes specially designed for operational risk. Accordingly, Basel Committee on Bank Supervision established the obligation that the coefficient (quotient) of regulatory capital should keep the level of at least 8% of its risk-weighted assets, i.e., 12% of the total capital requirement (Basel, 2003).

1. The importance of operational risk

The Basel Committee has recently reported an informal survey that highlights the growing realisations of significance of the risks that are neither market nor credit risks, but operational risks that have become the main cause for some important financial and business problems during the past couple of years. The following case histories are of particular importance (Gilett et al, 2010; Wang & Hsu, 2013): a) January 2008 – *SocGen* (€4.9 billion loss). A trader, Jérôme Kerviel, was systematically deceiving systems, taking unauthorised positions worth up to €4.9 billion in stock index futures. The bank had enough capital to absorb the loss, but its reputation was seriously shattered; b) February 2002 – *Allied Irish Bank* ($691 million loss). A trader, John Rusnack hid three years of losing trade on the yen/dollar exchange rate in the USA. The bank's reputation was damaged. c) June 1996 – *Sumitomo* ($ 2.6 billion loss). A copper trader piled up unreported losses over three years. Yasuo Hamamaka, known as "Mr. Five Per Cent", after the proportion of the copper market he controlled, was sentenced to prison for forgery and fraud. The bank's reputation was seriously shattered; d) September 1995 – *Barings* ($1.3 billion loss). Nick Leeson, a derivatives trader, piled up unreported losses over two years. Barings went bankrupt, etc.

Many of these spectacular losses can be traced to over ambitious and rogue traders or the cases of internal fraud. These failures include the mix of market and operational risks. The costs of such events can be quite high. They lead to large monetary losses, or even to bankruptcy. In addition to such direct costs, financial institutions often suffer great indirect losses due to reputational damage and lean development strategies. Perry and de Fontnouvelle (2005) found that, when operational loss is reported, market value of shares falls one-for-one with the losses caused by external events. They fall even more in the cases involving internal fraud, because the reason for that is weak internal control that causes further losses.

2. Risk implications

All the abovementioned oversights are symptomatic phenomena in the business environment. Some of them come as the consequence of the exposure to market or credit risks, but they are all, more or less, the consequence of inadequate operational risk management. Commercial banks are usually exposed to credit risk, less to operational and least to market risks. Investment banks, proprietary trading and financial management are mostly exposed to market risk. In contrast, retail brokerage and assets management are mostly exposed to operational risk. Consequently, financial institutions have created a formal structure for assessing and measuring operational risk. In particular, they are trying to define the economic capital (EC), which is needed to cover operational risk. The sums are not small, which reflects the importance of this type of risk. For instance, since 2009, JP Morgan Chase estimated that they needed $8.5 billion to cover operational risk, or 11% of total risk. The estimate of Deutche Bank was $3.5 billion or 17% of their total risk.

3. Operational risk identification

At a first glance, one could say that operational risk has no clear contents and definition in comparison to market or credit risk. A proper definition of operational risk or whether it makes any sense to try to measure it have been topics of long discussions. After much consultation, the Basel Committee formulated the definition that has become a standard in the financial industry and business processes. Operational risk is defined as "the risk of loss resulted from inadequate or failed internal processes, people and systems, or from external events" (Basel Comitte, 2006). It includes the common internal business events, but also the external ones like fraud, security violation, regulatory effects or natural disasters. Furthermore, it includes legal risk, which appears when it is proved that the transaction is legally inapplicable, while it excludes strategic and reputational risks which cannot be easily measured.

British Bankers Association (2008) provides even more detail. Table 1 (British Bankers' Association Survey, 2008; Bogojević Arsić, 2009) shows how operational risk is classified into four categories: people risk, processes risk, system risk and external risk. Among them we can notice a risk for complex products - model risk, which is due to the use of wrong models for estimating and managing risks. It belongs to internal risks that combine the lack of knowledge (people) with the complexity of products/estimation errors (processes) and possibly programme errors (systems).

Table 1: Operational risk classification

Internal risks		
People	Processes	Systems
Employee fraud	Accounting error	Data quality
Employee error	Capacity risk	Programme error
Employee misdeed	Contract risk	Security breach
Employer responsibility	Selling unsuitability	Strategic risk
Employment law	Product complexity	System capacity
Health and security	Project risk	System compatibility
Industrial action	Error reports	System delivery
Lack of knowledge/skills	Settlement/payment error	System failure
Loss or lack of important personnel	Transaction error	System unsuitability
External risks		
External		Physical
Legal		Fire
Money laundering		Natural disasters
External sources		Physical security
Political		Terrorism
Regulatory		Thieves
Supplier risk		Theft
Tax		

The Basel Committee has classified the risk events into seven different categories: 1) Internal fraud (IF): The events designed to defraud, property embezzlement and violating regulations or company policies, including at least one internal party, are categorized as unauthorized activities and internal theft or fraud. 2) External fraud (EF): The events designed to defraud, property embezzlement or violating regulations by a third party are categorised as theft, fraud or violation of security system. 3) Employment practices and work security (EPWS): The acts that are in discord with the employment, health or security regulations are categorised into the relations among the employees, environment preservation, diversity and discrimination. 4) Clients, products and business practices (CPBP): The events due to non-realisation of professional obligations towards clients, or arising from the nature or design of products, including revealing confidential secrets, improper business and market practices, product errors and advisory activities. 5) Damage to physical assets (DPA): the events leading to loss or damage to physical property due to natural disasters and other causes such as terrorism. 6) Business disruption and system failures (BDSF): The events that cause the disruption of business or system errors. 7) Execution, delivery and process management (EDPM): The events due to wrong processes of transaction or process management, stemming from the relations with traders and salesmen are categorised as maintenance and execution of transactions, customer documentation and accounting.

Furthermore, Basel II or The New Basel Capital Accord classifies the losses according to eight business lines : (a) corporate finance, (b) trade and sales, (c) retail banking, (d) commercial banking, (e) payment and settlement, (f) agency services and custody, (g) managing assets and (h) brokerage.

Both classifications have established the standards for defining operational risk events. These risk events are now collected, both internally and externally, according to the matrix of classification (for instance, according to event type or business line). This makes it easier to collect operational losses in the public databases. One of the examples is the Operational Risk data Exchange Association – ORX), which provides a platform for anonymous exchange of data on the operational risk losses, which is collected in ORX Global Loss Database.

4. Operational risk assessment

Being defined, operational loss should be measured, or rather assessed if it is more or less amenable to precise quantification in comparison to market or credit risks. There are various types of approaches and models (Rippel &Teplý, 2012) that can be broadly classified into the top-down or bottom-up models (Cornalba & Giudici, 2004). Top-down model attempts to measure operational risk at the broadest level, that is, using all the data relevant to the financial industry. The results are further used to determine the amount of capital that should be put aside as the shield against that risk. The capital is then allocated to business units. The bottom-up models start with individual business units or process levels, and the results are assembled to determine the risk profile of the financial institution. The main benefit of such models is that they lead towards a better understanding of the causes of operational losses, as in the case of a market, system risk based on the risk value (VaR).

The tools and instruments used for managing operational risks can be classified into several categories: a) Audit control. Such control consists of reviews and audit of the business processes by external auditors. b) Critical self-assessment. Each business unit identifies the nature and degree of operational risk. Such subjective assessments include the expected frequency and loss seriousness, but also a description of how the risk is controlled. The tools used for this type of process are lists, questionnaires and workshops. The results are then collected using the bottom-up approach. c) Key risk indicator. This approach consists of simple measures that provide indication if the risk is changing over time. Such early warning signs can include audit results, the staff turnover, the trade volume, etc. The assumption is that the operational risk is more likely to happen if these indicators increase. Such objective measures enable risk managers to envisage losses by applying regression analysis. d) Causal networks. The networks can be described as the losses that appear from a cascade of different causes. The causes and effects are connected through causal probabilities. Then simulations are initiated on the network where the loss distribution is created. Such bottom-up model can help understand the losses since they focus the risk initiators. Causal networks are best applied to the processes that include complex work flows with many activities. e) Actuarial models. Such models combine the distribution of loss frequency with their severity distribution to get the objective distribution of losses caused by operational risk. They can be either bottom-up or top-down models.

5. Actuarial models: loss distribution approach

Actuarial models assess objective distribution of losses from the historical data and are widely used in banking and insurance industry. Such models combine two types of distribution: The loss frequency and the loss seriousness. The distribution of the loss frequency describes the number of events that caused the loss over a certain period of time, called the Loss Distribution Approach (LDA).

The loss severity can be found in the table of historical data, for example measuring the loss strength γk at time k. These measures can be adapted to the inflation rate and certain measures of current business activity. If we define P_k as the consumer price index at time K, and γk as the measure of business activity such as the number of traders, we can assume that the loss seriousness is proportional to the business volume Q and to the price level. The proportional loss at time t can be presented as follows[4]:

$$x_t = \gamma_k \text{ x } \frac{P_t}{P_k} \text{ x } \frac{Q_t}{Q_k} \qquad (1)$$

Loss seriousness distributions have ma　　　　　　　nts, representing the possibilities for very large losses. It would be ideal if they could include both internal and external data. Internal data represent the real control environment in a financial institution. However, data are often insufficient or influenced by lame business of the bank that is still operating. Consequently, the data lack the accompanying elements necessary to model serious losses. In order to alleviate this problem, regulators demand the use of external data. These have deficiencies, as well. The scale and control systems of other banks do not always correspond to the bank using the data. The reports about operational losses to the external data base can be incomplete because some banks do not want to reveal their weaknesses completely. However, it is harder to hide greater losses. This makes the data collecting bias. Another deficiency is that databases only record losses above some minimum level, which can be as high as million euros, dollars or some other currency, which creates a bias in tracking distribution frequency and the loss seriousness.

In the further analysis we can calculate the loss frequency distribution by the variable n, which represents the number of loss repetitions over a period of time. The density function is as follows :

$$\text{p.d.f. loss frequency} = f(n),\ n = 0,1,2 \tag{2}$$

This can be described with several analytical functions such as binominal, Poisson, negative binominal or geometric, all of which require n to be a positive integer. If x (or X) represents the loss severity when a loss appears, its density can be defined as follows:

$$\text{p.d.f. loss strength} = g(x/n=1),\ = x \geq 0 \tag{3}$$

This can be described by the functions such as the lognormal, Weibull, gamma or exponential distribution, all of which need X to be positive. The most common combination is Poisson and lognormal.

The total loss over a period of time is given by the sum of individual losses over a random number of occurrences:

$$L_n = \sum_{i=1}^{n} X_i \tag{4}$$

Table 2 shows the simple examples of the two mentioned distributions that should be transformed into one – the total losses over the given period of time.

Table 2: The examples of loss frequency and the strength of distributions.

Frequency distribution		Severity distribution	
Probability	Frequency	Probability	Frequency
0.6	0	0.5	€500
0.3	1	0.3	€5,000
0.1	2	0.2	€50,000
Expected:	0.5	Expected:	€11,750

Assuming that the frequency and severity of losses are two separate variables, the two distributions can be combined into the distribution of total loss through a process called convolution. For example, convolution can be implemented through tabulation that consists of systematically recording all possible combinations with their associated probabilities, as illustrated in Table 3. Convolution should be implemented in a numerical method, since there are too many combinations of variables for systematic tabulation.

We start the analysis with the obvious case, with no losses, which has the probability 0.6 and then we go through all possible realisations of one loss only. From Table 3 we can see that a loss of € 500 can occur with total probability of P (n=1) x P (x = €500) = 0.3 x 0.5 = 0.15. Similarly, for one-time losses of €5,000 and €50,000 the probabilities are 0.09 i 0.06. Then we go through all the occurrences of the two losses that can result from many different combinations.

Table 3: Tabulation of Loss Distribution

Number of losses	First loss (€)	Second loss (€)	Total loss (€)	Probability	Sorted losses	Cumulative probability
0	0	0	0	0.600	0	60.0 %
1	500	0	500	0.150	500	75.0 %
1	5,000	0	5,000	0. 090	1,000	77.5 %
1	50,000	0	50,000	0.060	5,000	86.5 %
2	500	500	1,000	0.025	5,500	89.5 %
2	500	5,000	5,500	0.015	10,000	90.4 %
2	500	50,000	50,500	0.010	50,000	96.4 %
2	5,000	500	5,500	0.015	50,500	98.4 %
2	5,000	5,000	10,000	0.009	55,000	99.6 %
2	5,000	50,000	55,000	0.006	100,000	100.0 %
2	50,000	500	50,500	0.010		
2	50,000	5,000	55,000	0.006		
2	50,000	50,000	100,000	0.004		

For instance, the loss of €500 can appear twice, with total of €1,000, with a probability 0.1 x 0.5 x 0.5 = 0.025. Or, we can have a loss of €500 and €5,000 for total sum of €5,500, with probability of 0.1 x 0.5 x 0.3 = 0.15. We repeat these steps until we use up all the combinations.
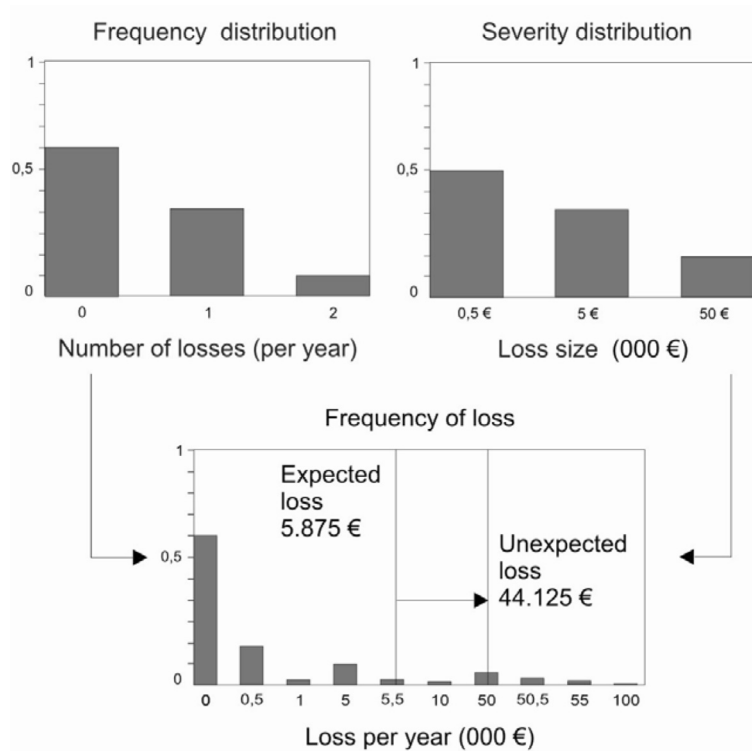

Figure 1: Construction of the Loss Distribution

The achieved distribution is presented in Figure 1, and in the lower part of Table 3. As usual in operational risk, losses are recorded as positive values. It is interesting to note that a very simple distribution from Table 2, with only 3 realisations, creates a complex data distribution. Therefore, we can compute the expected loss that is the product of the expected values for the two distributions, or

$$E[L] \times E[X] = 0.5 \times 11,750 = €5,875.$$

Risk management, however, concerns unexpected losses. So, the risk manager should report the lowest number with the probability greater than 95%. This is €50,000 with the probability of 96.4%. Hence, the unexpected loss is €50,000 - €5,875 = €44,125. If operational VaR must include the expected loss, it is simply €50,000. Basel II determined this to be the default measure, where VaR is 99.9% confidence level over one year.

6. Operational risk management

Just like the VaR, the distribution of operational losses can be used to assess expected losses by the amount of capital needed to support the financial risk as well. Figure 2 (Crouhy, Galai & Mark, 2010), shows the important characteristics of distribution of losses due to operational risk. The expected loss (EL) represents the size of operational losses that are expected to occur. This is usually dominated by high frequency, but low strength events. Such losses are usually absorbed as running costs and are managed through internal control. Such losses are rarely revealed.
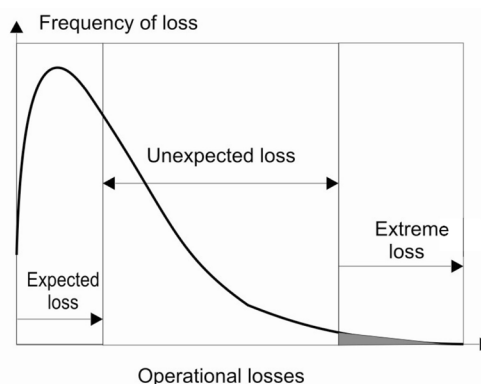
Figure 2: Distribution of operational losses

The unexpected loss (UL) represents a deviation between a quantile loss on a certain security level and the expected loss. These are typically low frequency and high severity events. Such losses are mostly alleviated by capital reserves or transferred to an external insurance company, if possible. Loss distribution approach can be easily modified if we take into account the risk-alleviating effect of insurance. The stress loss (SL) is an extremely severe loss that represents the loss exceeding the unexpected loss. By definition, such losses are quite rare, but devastating for the financial institutions. Therefore, the Barings bankruptcy can be largely attributed to operational risk. This type of loss cannot be easily compensated through capital allocation, as it would require too much engaged capital. Ideally, it should be transferred to an insurance company. Owing to their severity, such losses are revealed publicly.

7. alleviating operational risk

The approach so far has considered operational risk as part of business and something that should be measured. This information is very useful because it highlights the extent of operational risk losses. Having that information, financial institutions can decide whether it is worth spending funds on alleviating operational risk. Say that a bank is considering whether to install a direct process system that would automatically record trades in direct contact with the clients and send them to be processed. It would probably consider it worth, because such system eliminates manual interventions and potential human errors, thus decreasing losses due to operational risk. So, the bank should purchase the system if its cost does not exceed its operational risk benefit.

Generally, operational risk reduction can occur in terms of the frequency of losses and/or severity of losses when they happen. For instance, let's consider plain-vanilla swap transactions (Madura, 2010) with five-year interest. This simple financial instrument makes a large number of money flows; each of them has error potential. At the beginning, the purchase has to be booked and confirmed with the other party. Furthermore, profits and losses (π and L) should be estimated so that they could be attributed to a certain trading unit. With biannual payments, the swap will generate 10 cash flows together with 10 interest rate adjustments and payment computations. These payments have to be counted with absolute accuracy, i.e., to the last cent. The errors may vary from the minor ones, like paying a day late, to the major ones, such as the failure of traders to protect themselves against false assessments. However, swap will create some market risks, which may need to be transferred. The position should be transferred to the market risk management system that will monitor the entire system position and risk of the trader and the institution as a whole.

Operational risk can be reduced in many different ways, through internal and external control (Brewer, 1997). The methods of internal control include: a) Separation of functions. People responsible for committing transactions should not deal in ratification and accounting functions. b) Dual entries. The inputs from two different sources should correspond – trade ticket and back-office confirmation. c) Synchronisations. The results (outputs) from different sources should correspond: for instance, the trader's profit estimate and the computation in the middle office. d) Tickler systems. Important dates for transactions (e.g. balancing and the effect dates) should be entered into a calendar system that automatically sends messages before the due date. e) Control of amendments. Each amendment of the original dealer card must undergo the same strict

control as the original trade card. The methods of external control include: a) Confirmation: Dealer card must be confirmed with the other party, which provides unbiased control over the transaction. b) Verification of prices. In order to verify positions, the prices should be received from external sources. This means that the institutions should have the ability to internally value transactions before entering it. c) Authorisation. The other contractual party should be provided with a list of personnel authorised to trade, as well as a list of allowed transactions. d) Balancing. The payment process itself can show if some transaction conditions have been incorrectly recorded, e.g., if the first payment does not correspond across all the parties. e) Internal and external audits. These examinations provide useful information on potential weak areas in the organisational structure or the business process.

8. model risk

Model risk can be defined as the risk of loss due to inadequate price establishing or the inadequate pricing or risk measurement models. In a way, all the models are wrong. They are merely the abstractions of reality as Derman (2006) explained: "Even the best model is only a model of a phenomenon, not the real thing. A model is just a toy, often a very good one and it that case it is called a theory". Therefore, models are just approximations, or understanding of the conditions which make such approximations create unacceptable results. Figure 3 presents a taxonomy of the model risk sources. Firstly, the input data can be wrong, since they rely on the financial time series and other market data. The prices could be observed with error or could even be less important. Or optional inputs as the implicit business instability can be biased. Secondly, the model parameters can be inaccurately estimated. Risk models require descriptions of the statistical distribution of risk factors. These parameters are never precisely estimated. As a result, output values like VaR measures must contain some error. They can be reported on confidence bands, although this rarely happens. These bands should decrease with longer data series and shorter reliability levels for VaR. However, in some cases it is not possible to use longer series due to insufficient data or structural changes. Thirdly, the choice of a risk model can be incorrect. For example, for the options with fixed income, simple Black-Sholes model can be inappropriate. Alternatively, the mapping process includes the simplifications, which can prove wrong in certain cases. An example is a bank that mapped senior tranches of collateral debt obligations (CDO) supported by subprime loans on corporate yields graded AAA. This was done mostly for practical reasons, because of the absence of data on CDO yields. As a result, the bank thought that that these securities were risk-free and bought them in large quantities, only to realise billion-dollar losses later. Another example is the practice of mapping corporate securities and loan swaps on the same loan to the same input curve. Thus the basic risk was ignored, which caused some serious losses in 121 banks during 2008-2009. Fourthly, a model can be implemented inadequately. This can happen due to programme errors, to the selection of wrong parameters, etc. Model risk is difficult to identify and even more difficult to measure. That is all we can expect. Otherwise, errors would have been corrected in the first place. Risk managers rely on the *ad hoc* method in order to protect themselves against the model risk. Above all, they have to be aware of comparative strengths and weaknesses of different models. In other words, both intuition and experience are necessary.
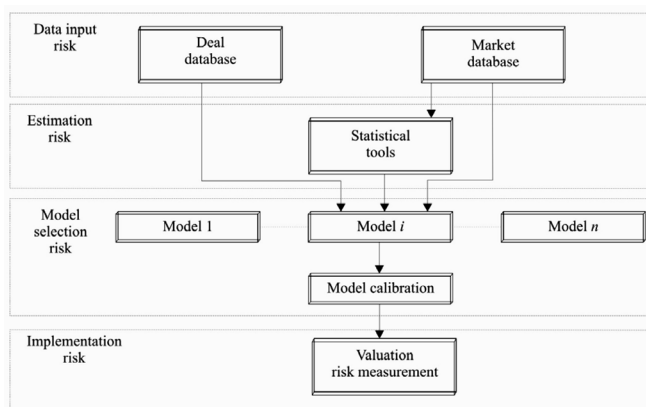

Figure 3: Model risk

Furthermore, they constantly need to estimate whether the key model assumptions are still valid. Then, a model should be tested against simple problems for which we already know the answers. Fifthly, the users should test the models by changing the input values to see if this substantially influences the output values. Besides, risk models should be also tested against actual data. This provides us guidance towards which part of the model can be improved.

For senior managers, the advice for decreasing operational risk is to be aware of the fact that the markets of new products and services can cause problems in model risk. These are the situations where risk models have not been fully developed because of time limitations or the lack of data. Besides, traders may deliberately damage the systems for monitoring risks to make their portfolio look more profitable and less risky. This is why the independence of functions is at the very heart of an effective risk management. Still, the measurement of operational risk is encumbered by conceptual problems. Namely, unlike market or credit risk, operational risk is of more internal character to the financial institutions. They unwillingly admit the mistakes they make while collecting data on operational losses, which creates new challenges for the risk managers. As we have seen, the internal data can be complemented by external data, but they can cause problems, too.

Extreme operational losses which can threaten the stability of a financial institution are relatively rare. That is why the number of observations is very small. Due to that problem, it is very difficult to reach the robust value for operational risk with a high rate of reliability. Furthermore, testing by the historical data is not as useful as the validation method. As for the market risk, VaR is usually measured on a daily bases and compared to daily profit and loss, which creates many observations for testing the risk model. On the contrary, the period is longer for operational risk, which creates fewer data for testing.

Conslusion

Measurement and monitoring of operational risk is different from other types of financial risks. The reason is the heterogenic quality of a range of factors causing operational risk which includes all the internal and external causes a halt of business. Due to the manner of their appearance and the moral hazard or negative selection related to the events from this range of factors, the probability to envisage them successfully is very low. Consequently, it is not possible to envisage the intensity of the financial impact they can cause.

Some types of operational risks can be measured (internal and external fraud or the "crash" of information systems). Other risk types (oversights in decision-making procedures, moral-hazard behaviour of the owners or managers in allocating assets, insatiable appetite for high profits and bonuses on one hand, and observing regulations on the other) are difficult to measure owing to their specific characteristics, insufficient data about these events and the fact they are inseparably integrated with other events from the group of phenomena that are typically called the negative selection. In order to manage, measure and identify operational risk it is of utmost importance that the current BIS definition of operational risk should be rephrased. IT risks are very complex, heterogeneous and volatile, so they objectively do not belong to this group. As such, they should be exempted and treated in a special way. After the IT risks have been exempted, the definition should be supplemented with the key factors that have influenced each of the operationally risky events, such as moral hazards and negative selection, since the uncontrolled development of operational risks has caused the appearance and spreading of the world financial crisis.

REFERENCES

[1] Basel Committee on Banking Supervision. (2003). Sound Practices for the Management and Supervision of Operational Risk.

[2] Basel Committee on Banking Supervision. (2006). International Convergence of Capital Measurement and Capital Standards. A Revised Framework. Comprehensive Version, June.

[3] Brewer W., (1997). *Minimizing Operations Risk.in Derivatives Handbook*. ed. Schwartz, R., and Smith,C.New York: John Wiley & Sons.

[4] British Bankers Association survey,(2008).

[5] Bogojević Arsić, V., (2009). Upravljanje operativnim rizikom u sektoru finansijskih usluga i novi Bazelski sporazum. *Management*. 59 (14), 15-22

[6] Cornalba, C. & Giudici, P. (2004). Statistical models for operation risk managment. *Physica A3378*, 166-172. doi:10.1016/j.physa.2004.02.039

[7] Crouhz, M., Galai, D.,& Mark, R., (2010).The Essentials of Risk Management. McGraw – Hill, 2010, 325 – 336.

[8] Dernan, E., (2006). *Model Risk*.New York: Goldman Sachs.

[9] Di Renzo, B.,Hillairet, M., Picard, M.,Rifaut,A.,Bernard, C., Hagen, D., Maar, P. & Reinard, D., (2007). Opeational Risk Management in Financial Institutions: Process Assessment in concordance with Basel II. *Software process improvment and practice*. 13.321-330. doi:10.100/spip.322

[10] Gillet, R., Hubner, G., & Plunus, S., (2010). Operational risk and reputation in the financial industry. *Journal of Banking & Finance*. 34, 224-235. doi:10.1016/j.jbankfin.2009.07.020

[11] Jorion, F., (2012). *Financial Risk Manager Handbook.* John Wiley α Sons.

[12] Madura, J., (2010). *Financial Markets and Institutions*, Thomson South-Western, 421-425.

[13] Marshall, C., & Siegel M., (2007). Value at Risk: Implementing Risk Mesurement Standard. *Journal of Derivatives*, 4 (3), 91- 111.

[14] Perry, J., & de Fontnouvelle, P., (2005). Measuring Operational Risk: The Market Reaction to Operational Loss Announcements. Working paper. Boston Federal Resreve Bank of Boston.

[15] Rippel, M., &Teplý, P. (2012). Overview of Operational Risk Management Methods. *World Academy of Science. Engineering and Technology*,70.

[16] Wang, T., & Hsu, C., (2013). Board Composition and Operational Risk Events of Financial Institutions. *Journal of Banking & Finance*. doi: http://dx.doi.org/10.1016/j.jbankfin.2013.01.027

[17] Wu, D., & Olson, D.L., (2010). Enterprise risk management: coping with model risk in a large bank. *Journal of the Operational Research Society*, 61**,** 179–190; doi:10.1057/jors.2008.144

/////////////////////////////////////// **About the Author**

Dejan Jednak
Privredna banka Beograd a.d., Beogra
E-mail: djednak@pbb-banka.com

Dejan Jednak holds M.Sc and B.Sc. degrees from the Faculty of Economics, University of Belgrade. He is a Ph.D. student at the Faculty of Organisational Sciences, University of Belgrade. He is employed at Privredna banka Beograd a.d. as the Head of Sales, Treasury Department.

Jovo Jednak
Belgrade Business School, Belgrade

Jovo Jednak holds a Ph.D. degree from the Faculty of Economics, University of Belgrade. He is a Professor at the Belgrade Business School, Belgrade. He teaches Economics and Financial Markets. He has published several books and scientific research papers.