UDC 005:658.14/.17 *Stručni rad*

MANAGEMENT WHEN SUPPLIERS' AND RETAILERS' RISKS BECOME COMPANY'S OWN RISKS

Nebojša Gijić[1], Dragana Banković Đukić[2], Adrijana Jović-Bogdanović[3]

[1]Faculty of Business Studies and Law, University Union-Nikola Tesla, Belgrade, SERBIA, e-mail: nebojsa.gijic@fpsp.edu.rs

[2]Faculty of Business Studies and Law, University Union-Nikola Tesla, Belgrade, SERBIA, e-mail: dragana.bankovic@fpsp.edu.rs

[3]Faculty of Business Studies and Law, University Union-Nikola Tesla, Belgrade, SERBIA, e-mail: adriana.jovic.bogdanovic@fpsp.edu.rs

Abstract: *Risk in business refers to a smaller or greater uncertainty regarding the expected outcomes of business activities. Modern practice of management of complex business systems, among other things demands also risk management of many business processes and potential damage that may arise in the course of business. The point is uncertainty of changes in business conditions and insufficient and unreliable information on the basis of which to make business decisions. The key to successful risk management is to clearly define the areas of risk assessment, identification and registration of potential hazards that can cause events with negative consequences and a thorough understanding of all aspects of these consequences. By introducing insurance of assets and other resources likelihood of damage is significantly reduced.*

Keywords: *management, risk, suppliers, retailers, consumers.*

1. INTRODUCTION

The term "supply chain management" has emerged as a result of the way of observing the whole process of supplying the customer with products that he needs. Observation begins from the end of the physical processes of supply: from the purchase, i.e. from the customer. The buyer is interested in the product, that product is sold by the seller, who bought the product from a distributor, who got it from a manufacturer, who had to procure raw materials and intermediate products of the product, from the vendor. Each participant in this series represents a link that connects the source of raw materials to customers.

Earlier risks had disappeared, but were replaced with new risks associated with progressing technology. Many risks facing business today were unknown to former generations

of people. Some of them are arising from changes in legal regulations and include the possibility for plenty of new offenses in the form of environmental pollution, discrimination and violence in the workplace. Some risks simply accompany urgency of today's information technology - interference in business because of computer errors and embezzlement by a computer. Bandits and pirates who used to be a threat to the former traders were replaced by hackers who are involved in computer vandalism and make electronic theft.

The term 'risk' implies the risk of exposure to the unfortunate circumstances. The definition of risk varies from one discipline to another, and even in the same area there are some contradictory definitions. Risk is a condition in which there is a possibility of dangerous deviation due to the danger of desired outcomes that is either expected or desirable.[1]

Risk control techniques are designed to minimize, as much as possible, those risks to which organizations are exposed. Control methods include avoidance of both risks and various mistakes, as well as reduction of risks through prevention and efforts to establish control. In the case of risk aversion, individuals or organizations refuse to accept any exposure to loss from certain activities. Although risk can be reduced, it can never be completely eliminated.[2]

Risk reduction consists of all the techniques that are designed to reduce the possibility of loss, or the potential hazards of those losses that eventually occur. It is widely accepted that there are differences between preventing losses from those efforts that serve to prevent losses from happening and to minimize loss, efforts that serve to reduce the risk of loss if they occurred.

It is not adequate to talk about one single aim of risk management just as it is inadequate to speak of one single goal of any business or any organization. Most organizations will have multiple objectives, and most of the functions within the organization will have more goals. The objective of risk management must represent inherent uncertainty in a situation of risk management. Exactly because one should know that losses will happen and what will be the total sum of such losses, preparations are made to ensure survival in the event of a loss, and they must reflect the worst possible combination of outcomes.

2. RISK IN THE CURRENT BUSINESS ENVIRONMENT

Risk is defined as the possibility of suffering harm or loss, respectively: a factor, thing, element that involves uncertainty and risk.[3] The concept of risk not only changes, but also varies depending on the segment of human life and activity, and as such is differently defined and evaluated. Risk is defined as the effect of uncertainty on objectives. There simply cannot be positive or negative risk, but only risk as such. The risk poses the problems in the future that can be avoided or mitigated unlike the current ones, to which we must respond immediately.

A company that observes its operations in an isolating way, without networking with other strategic players in the supply chain in advance is doomed to failure. Even those companies that indeed engage in the contemporary market trends are not guaranteed survival, but the spirit of change must be integrated within the company so that this new "mantra" becomes a strategic and operational driver of the business fronts at all times.[4]

Risk assessments are carried out regularly, while evaluations can be performed periodically, taking into account possible changes in the factors affecting the risk and environment.

This requires good cooperation between all parts of the organization and administration levels. Organizations are taking measures to manage risk in the following manner:

- The adoption of strategy for identifying risks.
- The application of appropriate corrective measures for the prevention, management and treatment of identified risks.
- The implementation of internal control procedures.
- Regular assessments of risks, including monitoring of the level of risk in order to determine trends based on the frequency.
- Monitoring of the audit findings and other controls in order to identify new possible risks. [5]

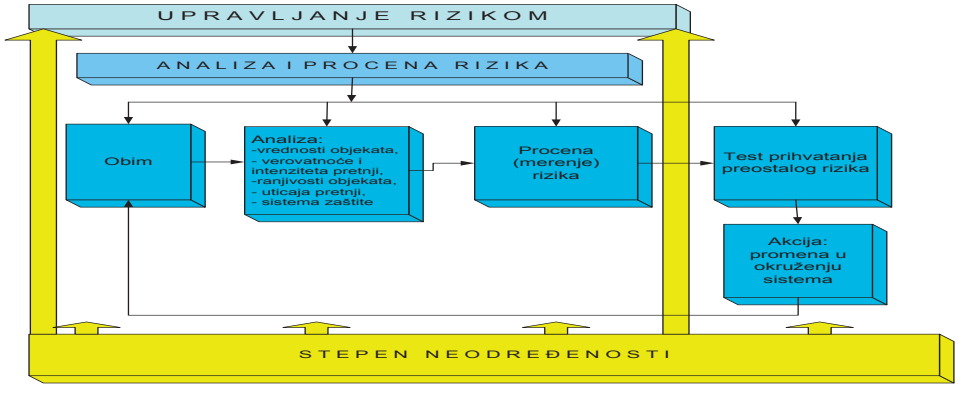

Figure 1: The general model for the analysis and assessment of risks

The theme of risk is indeed actual across all markets, but not treated equally. For example, in America, according to a survey conducted by *Navex* (Navex Global is a recognized agency that provides services to harmonize software, content and services, collaborating with over 8,000 customers in 200 countries), it was found that fewer than 3 in 10 US companies follow closely its third-party vendors, suppliers and associates to prevent corruption, fraud and other compliance risks.[6] This survey was conducted in September 2013, just after the US Justice Department said that in 2012 more than 90% of its anti-corruption activities focused on companies involved in relationships with their third parties. Let us mention the case regarding *Glako Smith Kline* in China, where Chinese police accused the British drug manufacturer (GSK), that the money used to bribe Chinese officials and doctors, hospitals, was directed in through at least 700 tourism agencies, in order to illegally instigate sales and raise prices of their medications in that country. The case is still under investigation. Further, this study showed:

- Only 29% of US companies monitor the connection of their third party.
- The majority of respondents (85%) into the list of key issues include bribery and corruption.
- It is expected that companies increasingly rely on third-parties to assist them to meet their objectives of income and services.

- More than a third of them believe that they do not have the tools to reduce the risk of a third party and compliance risks.[6]

3. MANAGEMENT BY RETAILERS AND SUPPLIERS OF THEIR OWN RISK

Financial institutions are responsible for the actions of their suppliers. The new approach can help identify causes of risk management and third parties. The rising tide of regulatory oversight arising from the global financial crisis and is now reaching even beyond banks and companies that supply them. In a broader sense, these activities may be external, but responsibility cannot. Consumer Financial Protection Bureau (CFPB) and other regulators of financial institutions are held accountable not only for their own actions (work), but also for those who supply them and perform sales for them. Last year, for example, American Express, Capital One and Discovery Bank paid more than $ 530 million to cover appeals for fraudulent sales and predatory behavior by their third-party sellers.

This new regulatory pressure is a major challenge for the Financial Institutions, because some of them have a limited view of the mutual influence of their suppliers and customers. Major banks and credit card companies may have nearly 50,000 suppliers. They are very careful regarding some of these connections (relations), and often have teams to manage large and medium-sized suppliers. Of course, many sellers provide papers, computers and other innocuous goods and services. However, a significant number of the seller relations are not carefully implemented, and carry some hidden risks. Companies that process and print credit cards, for example, are given data on customers; this leads to endless confidence and security risks.

In many institutions, programs of commercial management are mainly focused on the risks to the banks and the financial system - specifically, business continuity, financial stability, and credit risk. Many companies are simply unprepared for the expansion of regulatory oversight that includes customers. But, since financial institutions must be held accountable for violations made by their suppliers, they have to improve their way of managing these relationships.

In response to changes, financial companies are looking for new solutions to identify and manage risk by third parties. The number of leading banks and companies for making credit cards grow and they continuously adopt best practices. Current research and experience helps to develop a comprehensive approach to risk management by third parties. It consists of six basic steps, some of which can be executed in parallel. [7]

1. A comprehensive list of third parties. Regulators (editors) now expect that institutions know their third parties, as each of them is to interact with consumers; they must know exactly what activities they perform. Many companies have no readily available data. Supplying databases may be incomplete, and some of the most sensitive risks can be found in relationships that are not found in them. Community partnerships, joint ventures, sponsorship, and similar concerns can amount to 80% of the costs that some business units have with suppliers. However, often these relationships are managed in a way to emphasize commercial purposes, and only with a secondary focus on risk. Moreover, in some companies, the individual entities have different ways of monitoring their suppliers, as a real difficulty in comparing and reviewing the level of the entire organization. Efficient database of third parties includes all of them, i.e. includes each and every customer with whom the financial institution has a business relationship.

2. A comprehensive directory of independent risks. For successful monitoring of consumers risks, firms must develop a comprehensive catalog of these risks, among other things, known as black points that form the basis of the overview of the results, standard reports and other monitoring activities. Let us consider a black spot in the third-party call center if there is a risk that agent falsely presents product to the client. The bank can investigate this particular problem by monitoring calls and may require regular reports on their quality at the customer's request (in writing). Marking relevant black points for each category of suppliers and determination of the relative weight and value and importance of each breakpoint can definitely prove to be a challenge. Creating a master registry of black points and their associated risk measurement for all categories can be helpful. Although it is applicable to most companies, master registry can be adapted to specific conditions of individual organizations and their unique relationship with a third party. This process is essential, as it helps the company to identify the main drivers of its risk and lead to their fall.

3. Segmentation based on risk. Once the company has a complete inventory of independent suppliers and customers risks, it can divide their suppliers by risk level. Even a simple system of categorization of high, medium and low risk can be beneficial. It was noted that most of the leading institutions have 200 to 300 high-risk relationships at the same time, regardless of the total number of third parties with whom they have contracts. An effective segmentation (division) can help companies to strategically engage their resources. This way they can, for example, take an additional procedure at high-risk relationships and automate regular checkups low-risk suppliers.

Evidence of input	*Volume of debtors*	*Account maintainance*	*Payments*	*Evidence of output*
Files not transferred, information about the debtor incorrect. • Incorrect classification of files.	The feature does not fit into the window of permitted telephone contacts - time determined by FDCPA *. Agents use derogatory words and incorrectly state the facts (e.g. exact debt). • Agents continue to contact debtors despite written dispute. • Agents come into contact with debtors represented by lawyers. • In communication they fail to inform debtors that they have the right to dispute the debt.	The Agency takes actions that are not guided from the bank or do not receive authorization. The Agency does not inform the bank about the account activity and important events (e.g, bankruptcy). The Agency does not submit verification of the debt or a copy of the judgment against the customer, regardless of their requirements.	Payment incorrectly applied and set. Borrower erroneously reported payment information Debtors' payments may not register. Some automated payments cannot be complied with. Failure to mark payments on closed accounts; unidentified payment.	Files are not correctly transferred to other agencies and back to the bank. No reports on the activities undertaken in cases. Confidential info about the borrowers are not completely removed from the agency.

Figure 2: To reduce risk, companies need to adapt supervision of specific critical points[7]
Example: The black points of a third party call center in the United States have been selected
* Violation of US law on debt collection (FDCPA)

Companies typically use one of two approaches to divide third party suppliers. Companies that follow the approach based on the results, conduct due consideration to all measures and use the results to develop complex sources of risk. Although very thorough, this approach can be a laborious and intensive asset for many organizations. Using the principles of

the basic rules, the company identifies specific rules and criteria for each part, and thus simplify the process of assigning supplier risk categories. In fact, this approach is approximately 40 to 60% faster than an approach based on results. Given the importance in the approach to segmentation, leading institutions tend to further invest in designing them. Typically, they determine the core team of experts for risk, which manage design, fine-tuning and implementation.

4. Test of professionalism based on rules. Today, companies expect to expand their business efficiency beyond the traditional assessment for suppliers, operational risk and IT security. Regulators are particularly sensitive regarding strategic and renowned risk that a third party can make to customers. The traditional approach equates professionalism specific activities with risk category which it recognizes on the basis of risk sharing. A supplier in the high risk category of risk is subject to all aspects of the investigation. Also, as an approach based on results, this concept can be very difficult and intense. Here also, a better response can be accessed on the basis of the rules, because it activates an appropriate set of business activities for risk identification. For example, even when you consider that a third party presents a high risk, control of information security and privacy of data is not necessary if the supplier does not possess information that personally identifies customers. By accessing the Rules, one can save time of the employees by almost 40%.

5. The disciplined management and escalation process. Organizational guidance is especially important when the right decision-making spread across different business areas and functions, such as procurement, service and operational-risk management. By proactively establishing a management structure and processes for resolving discrepancies, institutions can quickly solve the challenges.

Management can be centralized or decentralized; both models (and some hybrids) can be successful. In the centralized model, the majority of high-risk decisions are in one group, such as the purchase or sharing services. Regardless of the fact that centralized model recognizes clearly the responsibility of the "owner", it can sometimes lead to tensions between the business unit that has a working relationship with a third party and a centralized body responsible for risk assessment.

In a decentralized model, the business unit that uses the relationship is also tasked with managing the risk. This arrangement can sometimes lead to duplication of resources: several business units may, for example, to assess the main third-party vendors for similar contracts. In some cases, the application of standards and harmonization of risk may be contrary to the decentralized model: the control group, according to supply and (driving) operational risk may have a different perspective. The hybrid approach, carefully tailored to organizational context, can help to mitigate the challenges between the two models until the owner of the known risks.

Extension of the scope is crucial for solving issues - such as requests for exemption and resolving delays by third parties - that go beyond the area of decision-making said management structure. While most organizations have operational risk management, their governance model and powers may not be sufficient to solve the additional scope of issues related to third parties. Leading financial institutions often prefer to assign new responsibilities to standing Committees but to create new support expansion of third parties. Each organization needs to find an appropriate approach in view of its risk assessment and its culture.

6. The process of integrated management reporting, work process and tools. Clearly, effective managerial reporting and well-designed process systems are essential for accountability across all business units, their regularity and auditing. To perform well, these tools

need to find and keep track of relevant information. More importantly, they need to assist the monitoring of work processes within and across business units and managers provide a clear picture of the risk in real time, with concrete proposals. Most organizations now have tools to solve one or two of these functional processes; still, it is a well-known fact that no one has a unique tool that covers all three processes.

4. CONCLUSION

Companies pay most attention to the financial-commercial moment, development, business continuity, credit risk, as well as to the risk regarding banks. Many companies are targeted by fraudulent sales, and predatory behavior of third parties. Extending of regulatory supervision must include all those involved in the process. Risks of retailers and suppliers represent a significant challenge for financial institutions. Systematic approach to management of these risks can reduce costs and help banks in presenting a consistent approach to all key stakeholders, including the regulators (editors).

Financial institutions are responsible for the actions of their suppliers. The new approach can help in identifying and managing sources of independent risks. The tide of regulatory oversight has expanded beyond banks, to companies that supply them. Financial companies are looking for solutions to identify and manage independent risks. Construction of new applications risk of third parties from the start is a major undertaking indeed. The same applies for the improvement of risk tools in terms of performing new functions. Some companies have turned to commercial tools – and means for risk management, which can easily be adapted to the specific needs of an organization.

Companies must develop a catalog of risk known as the turning point, which forms the basis for the assessment of cards, the audit routines, and other monitoring activities. Building a master registry counts interrupts and their associated risk weight for all of these categories, can be of great help. Master registry can be adapted to individual personal circumstances of the organization and unique independent connections.

Effective segmentation can help firms determine how to strategically use its resources. Reports of active management and well-designed flow systems are essential for accountability at the level of each business unit, and the regularity audit.

It is not enough merely to establish different functions that will address risk management and control - the challenge is to assign specific roles and effectively co-ordinate them in a way to avoid the "holes" in the controls, and the unnecessary duplication / overlap. The competencies must be clearly defined, so that every function that has jurisdiction over these issues understands the boundaries of their own responsibility and is aware of how its position fits into the overall organizational structure in terms of risk and control.

BIBLIOGRAPHY:

[1] Radosavljević Ž., Tomić R. 2007., Menadžment u modernom biznisu, Novi Sad, Privredna Akademija, 84.
[2] Šabović Š. 2012.„Otkrivanje rizika u poslovanju preduzeća", Novi Pazar, Socioeconomica, Vol 1, br 2, dec 2012., 221.
[3] Živković Ž., Savić M., 2013., Upravljanje rizikom,Bor, Univerzitet u Beogradu, Tehnički fakultet u Boru, 4.

[4] Mijušković Veljko2010..„„Revolucionarni poslovni trendovi u upravljanju lancima snabdevanja“, Beograd, Ekonomski fakultet u Beogradu, Časopis Marketing,Vol. 41, br. 1, 54.
[5] Džunuzović E.., Priručnik za upravljanje rizikom i procenu rizika u javnom sektoru,Podrška razvoju interne finansijske kontrole u javnom sektoru – faza 3, Srbija, Safege, Projekat finansira EU, 9.
[6] NAVEX anketa 2013., http://www.navexglobal.com/company/press-room/navex-global-survey-7-10-us-companies-neglect-third-party-risk.
[7] Samandari Hamid, Walsh John, Yueh Emily 2013., Managing when vendor and supplier risk becomes your own, McKinsey Quarterly, July 2013., http://www.mckinsey.com/insights/risk_management/managing_when_vendor_and_supplier_risk_becomes_your_own