ORIGINAL RESEARCH PAPER
Volume - 11 | Issue - 06 | June - 2022 | PRINT ISSN No. 2277 - 8179 | DOI : 10.36106/ijsr
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

FINANCIAL RISK MANAGEMENT

Management

Dr.V.sivakuamr Professor, Department of Mba, Jayam College of Engineering And Technology, Nallanur , Dharmapuri – 636813

Mr.Manjunathan K* Mba Final Year Student Jayam College of Engineering And Technology,nallanur, Dharmapuri - 636813*Corresponding Author

ABSTRACT

This paper analyses financial risk management at the Ministry of Defense of the Slovak Republic. In its first part, the author defines the basic terms related to risk management, explains the negative consequences of risks and points to the importance of financial risk management. The second part of the paper is concerned with the risk management process at the Ministry of Defense of the Slovak Republic relating to financial management.

KEYWORDS

financial resources, financial risk, management system, organization of the public sector, ministry of defense

1.Introduction

Life and all human activities involve a lot of existing risks and various crisis situations that can produce detrimental effects. survival of risks results from the fact that every human activity is associated with potential loss, failure, damage and disruption of stability or security.

Since economy is subject to continuous change, each organization has to deal with existing risks in real environment and real time. Financial management in organizations with various risks, which have an impact on running and existence of private and public Companies.

Management of scarce resources in both types of organizations involves the same rules of economic rationality. Managers in private and public companies have to deal with similar risks, but also the risks that are connected with specific activities and different financing methods.

Even though the public demands reduction of financial resources allocated to public organizations, services provided the public must not be restricted. Revealing the risks associated with financial management in public institutions is not sufficient.

It is necessary to adopt adequate preventive measures, or in other words, to manage the risks using the systems approach. Revealing the risks associated with financial management in public institutions is not sufficient.

Define the risk of a portfolio as its variance through diversification portfolio optimized so as to achieve the lowest risk for a given targeted return, or equivalently the highest return for a given level of risk. these risk-efficient portfolios form the "Efficient frontier" Markowitz model.

The logic here is that returns from different assets are highly unlikely to be perfectly correlated, and in fact the correlation may sometimes be negative. In this way, market risk particularly, and other financial risks such as inflation risk, can at least partially be moderated by forms of diversification. Financial risk is a type of danger that can result in the loss of capital to interested parties. For governments, this can mean they are unable to control monetary policy and default on bonds or other debt issues. Corporations also face the possibility of default on debt they undertake but may also experience failure in an undertaking the causes a financial burden on the business.

Financial markets face financial risk due to various macroeconomic forces, changes to the market interest rate, and the possibility of default by sectors or large corporations. Individuals face financial risk when they make decisions that may put at risk their income or ability to pay a debt they have assumed.

Financial risks are everywhere and come in many shapes and sizes, affecting nearly everyone. You should be aware of the presence of financial risks. Knowing the dangers and how to protect yourself will not eliminate the risk, but it can mitigate their harm and reduce the chances of a negative outcome.

Volatility brings uncertainty about the fair value of market assets. Seen as a statistical measure, volatility reflects the confidence of the stakeholders that market returns match the actual valuation of individual assets and the marketplace as a whole. Measured as implied volatility (IV) and represented by a percentage, this statistical value indicates the bullish or bearish—market on the rise versus the market in decline—view of investments. Volatility or equity risk can cause abrupt price swings in shares of stock.

Default and changes in the market interest rate can also pose a financial risk. Defaults happen mainly in the debt or bond market as companies or other issuers fail to pay their debt obligations, harming investors. Changes in the market interest rate can push individual securities into being unprofitable for investors, forcing them into lower-paying debt securities or facing returns. Speculative risk is one where a profit or gain has an uncertain chance of success. Financial risks not inherently good or bad but only exists to different degrees.

2.Financial Risk Management System Adopted at the Ministry of Defense of the Slovak Republic

The public in Slovakia increasingly calls for effective management of public organizations and reduction of risks associated with management of budgetary resources. Public organizations that manage budgetary resources are supposed to obey the act on budget rules, develop a functional system of risk management and respect the "value for money" principle while carrying out public procurement.

The European Union accession procedure requires risk management legislation as an obligatory standard. Therefore, the Ministry of Finance of the Slovak Republic issued the "Regulation on Risk Analysis and Management in Public Administration" in 2006 (Oláh & Šidelský, 2017). Financial managers in public institutions in the Slovak Republic are expected to adopt measures that will ensure effectiveness of performed activities and eliminate cost inefficiency.
The Act No. 357/2015 Coll. on Financial Control and Audit, which came into force on 1 January 2016, obliges public administration bodies to manage public finances efficiently, firmly and effectively. Pursuant to this act, risk management process is an essential part of financial management, which the public administration body, including the Ministry of Defense of the Slovak Republic, is supposed to maintain, develop and improve continuously. In arrange to fulfill this requirement, the ministry adopted an internal regulation on "Financial Risk Management", which has been in force since 2017.

Pursuant to this regulation, financial management is a set of procedures that the Ministry of Defense of the Slovak Republic adopts in risk management, responsible planning, budgeting, use, allocation, accounting and reporting of public finances as well as financial control and internal audits. capable purposeful and effective use of public finances. Financial and process management includes also risk management as one of the management tools the ministry uses to achieve its goals.

As previously mentioned, financial management of a public organization may involve certain risks that can have a negative effect

on its goals and tasks. Every employee (not only the executive staff), who identified a major risk that could have a substantial impact on public finances and fulfillment of tasks and goals of the Ministry of Defense of the Slovak Republic, is obliged to immediately, The Slovak Republic must be prepared to react to a wide spectre of existing and potential threats.

At the same time, it is aware of the fact that threats and attacks emerging in cyber space may escalate up to a level that would require collaboration of the allies within the North Atlantic Treaty Organization (hereinafter referred to as "NATO") under Article 5 of the North Atlantic Treaty1 that would result in a collective defense and/or coordinated response. Thus, cyber security also needs to be perceived as a subsystem of national security and cyber space as its new operational domain. The Slovak Republic intends to cooperate with all relevant state and private cyber space actors, which respect identical values and do not restrict the freedom and safety of the use of cyber space.

Economic efficiency is the use of public finances for performance of activities or purchase of goods, works or services in appropriate time, amount and quality for the best price. Keeping the costs down is monitored. Financial audits check whether the specified goals were fulfilled by means of the most suitable inputs and the lowest possible costs. *Effectiveness* is the best possible relationship between costs and outcomes. It is an attempt to achieve the maximum from available resources. Financial managers need to ask themselves a question – "Are the things done properly?" *Efficiency* can be described as fulfillment of specified goals and achievement of planned results by means of public finances. Managers answer the questions – "Are the things being done properly? Are we achieving the defined goals and results thanks to the financial resources that we are using?". Efficiency is determined by comparison between what should have been done or achieved and what has been done or achieved. Consideration is a relationship between the defined purpose of public finances use and the real purpose of their use. The outcome of costs must always be performance of specific usefulness. Financial audits determine whether public finances were used for what they were allocated.

Risk is the probability of occurrence of an event that will have adverse effects as far as the running, finance, legal matters and fulfillment of goals and tasks are concerned.

Ineffective or purposeless use of public finances, non-compliance with generally binding regulations, failure to fulfill the tasks that can threaten achievement of specific objectives, performance of ineffective or purposeless activities, performance of activities that are beyond existing competencies, non-compliance with the required quality.

Other negative influences include threats to information and information systems security and overall damage to organization's good reputation (Oláh & Šidelský, 2014).

Risk *management* is a recurring process of interrelated activities within financial management that are aimed at controlling a possible risk occurrence.

The goal of risk management is to decrease the probability of risk occurrence, reduce impacts of the risks and prevent bad results and negative phenomena in entities belonging to the defense sector.

Responsibility for risk management lies with the executive staff of the defense sector the Minister of Defense of the Slovak Republic, the state secretary, the head of the Service Office, the Chief of the General Staff of the Slovak Armed Forces, executives who manage individual sections military units, military offices and installations and other managerial immediately personnel.

Advise the head of a particular section of the risk occurrence. This employee adequately responds to existing or detected risks and immediately advises the executive staff of the risk occurrence in a written or oral form.

It means that the personnel responsible for risk management include both civilian employees as well as professional soldiers who manage the defense sector. The Concept is based on a statement and a description of the basic terms and principles, characteristics of the current situation of the strategic, legal and institutional frameworks in the area of cyber security in the Slovak Republic and on a strategic and methodological framework formed by NATO and European Union (hereinafter referred to as the "EU") documents; subsequently, the Concept formulates principles, goals and proposed solutions. .

The relation of cyber security to the basic security areas of operation of the state and the mutual relation between cyber security and information security are discussed in the following chapter of the Concept.

Cyber security is one of the defining elements of the security environment of the Slovak Republic and a subsystem of national security. At a state level, it is a system of continuous and planned increasing of political, legal, economic, security, defense and educational awareness, also including the efficiency of adopted and applied risk control measures of a technical-organizational nature in cyber space in order to transform it into a trustworthy environment providing for the secure operation of social and economic processes at an acceptable level of risks in cyber space. The Slovak Republic still lacks a consistent formalized terminology in the area of cyber security. The word cyber and its other grammatical forms do not occur in any generally binding regulation nor in terminological dictionaries cyber security, cyber space, national cyber space for the purposes of this Concept..

For the real performance of state administration in the area of cyber security and to understand the relationship between cyber security.
The Slovak Republic is fully in line with the principles of cyber security precise in the strategic document "Cyber security Strategy of the European Union"7 as well as with the principles specified in the "Enhanced NATO Policy on Cyber Defence"8.

3. Financial Risk Management Process at the Ministry of Defense of the Slovak Republic

In terms of theory, risk management is a systematic application of managerial policy, procedures and experience in the following activities According to the internal regulation, the risk management process at the Ministry of Defense of the Slovak Republic consists of the following steps:

- identification of risks,
- analysis and assessment of risks,
- treatment of risks,
- monitoring of risks,
- assessment and verification of the risk management process.

Risk identification determines to what extent the fulfillment of objectives is endangered due to uncertainties resulting from possible negative effects. This step includes reports and notifications of risks that provide information on the risk source and bearer. This information is essential for adoption of adequate measures. Risk identification is done by means of various methods and it is based on expert judgment and knowledge of the field in which the risk has been identified. The outcome of this step is description of the risk, which is then recorded in the risk register. This in turn informs considerations about whether the risk is avoidable or insurable; the extent to which it can be mitigated; whether it can be shared; and what role public administration should play in managing it.

Risk analysis and assessment is a prerequisite for making decisions on how to treat the risk. It is performed according to widely used models and procedures or their combination for example, market research, search and modeling of real possibilities,

Risk assessment provides information on how serious the risk is, whether it can be accepted or if it is necessary to adopt measures to treat it. Financial risk management uses a three- level scale to assess the risks.

The scale includes the following criteria:
likelihood (frequency):

- low level 1 – occurrence of the risk event is rare or possible.
- medium level 2 – occurrence of the risk is possible and the risk event frequently recurs.
- high level 3 – occurrence of the risk is highly likely or even certain, the risk event often recurs.

low level 1 – consequences are not serious and financial loss is minimal the consequences have no or only a negligible impact on the ministry's objectives however, if appropriate measures are not adopted, these risks may bring about more substantial and cumulative effects there is an extremely human activities covered by the Sustainable Development Goals.

medium level 2 – risks can have more significant effects of the ministry's objectives they usually occur irregularly and they are not easily predictable.

High level 3 – risks may enormously influence accomplishment of the ministry's objectives and they can cause huge financial losses or other kinds of losses; they usually occur irregularly and they are not easily predictable.

The outcome of this phase is determination of a significance level of the risk, which is recorded in a risk register, risk catalogue and a risk map.

Risk treatment means adoption of measures in order to minimize the occurrence or reduce the influence of a possible risk. It is the process of selecting and implementing of measures based on evaluation of alternative appropriate actions (avoiding the risk by adopting other measures, removing the risk source.

Reduction of likelihood and direct consequences of the risk, passing on the risk to another entity, e. g. by means of insurance, accepting the residual risk). In risk treatment, much attention has to paid to the medium (points 3 to 4) and, especially, high (points 6 to 9) significance level of the risk.

Risk mitigation measures must be adopted on the basis of estimated cost- effectiveness. Risks at low implication level that do not require adoption of any measures are deemed to be acceptable.

Risk monitoring and assessment is the flow of information on the risk management results at a particular organizational section – a risk owner.

It includes submission of evaluation materials, which contain information about control activities focused on risk management, adoption of mitigation measures and assessment of their effectiveness. The output of this step is the information on treatment of serious risks in strategic and evaluation materials, which is presented at sessions of chiefs of individual sections and executive staff of the defense sector, and the internal audit reports.

Frequency and size of impact. This is a common distinction in insurance. The characteristics of each risk influence the ways in which it can be addressed by individuals, communities, the private the state. In all fields, risk management is conceived as a sequence of stages, going from identification of potential risks to analysis and assessment to response to monitoring and evaluation.

The nature of the risk under scrutiny, the specific phase of treatment, the availability of resources, regulatory requirements, administrative norms and sector specificities will ultimately determine the appropriate risk management techniques that can best support risk management.

4.Risk and the Sustainable Development Goals

This section briefly surveys the intersections of risk and the 2030 Agenda and the SDGs. After providing working definitions for this chapter, it examines broad considerations for risk management in public administration, which were used to inform the scope of the chapter. The chapter then reviews how risk is addressed in the text of the Agenda and the SDGs, and contrast this with an examination of risks-related issues in various SDG areas, based on examples as well as a review of the academic literature.

National examples of risk management in public administration This section illustrates how risk management is institutionalized in public administration in various countries. The goal is to illustrate a variety of techniques and tools employed in managing diverse risk types in different SDG or nexus areas.

Advanced technology is used to manage risks associated with malicious use of technology itself. Emerging digital and cyber security risks are a case in point. In September 2018, the United States Government established the National Risk Management Centre (NRMC), as a subcomponent of the National Protection and Programs Directorate of the Department of Homeland Security. NRMC has evolved out of the former Office of Cyber and Infrastructure Analysis. Its mandate is to advance the understanding of emerging cyber physical risks. The NRMC plays a key role in the Department's work to implement Presidential Policy Directive 21, which calls for integrated analysis of critical infrastructure, and Executive Order 13636, which identifies critical infrastructure where cyber incidents could have catastrophic impacts on public health and safety, the economy and national security,

well as knowledge of public finance management (Petrofina, 2014). Therefore, there has to be a methodical basis that professional soldiers can rely on in the risk management process.

The Ministry of Defense of the Slovak Republic responded flexibly to this requirement by adopting an internal regulation on financial risk management. organization of the framework for financial risk management should enhance the quality of management in internal organizational.

Risk-based decision making is increasingly used in environmental management, and risk-based regulation has emerged as a tool of natural resource management Both disaster and emergency management and climate risk management imply cross-cutting risk analysis connecting several sectors, within and beyond ecosystem management. LEAP converts satellite and agro-meteorological data into crop or rangeland production estimates and derives livelihood protection requirement.

Conclusion

Risk management is becoming increasingly important also in management of public organizations. Professional soldiers working as managers have to be competent in many areas. They are supposed to have military knowledge as sections of the defense sector and support the cost-efficient and effective budgetary policy, maintenance of financial and budgetary discipline and rational spending of public funds for ensuring national security.

Methodical instructions concerning risk management in public organizations (including the defense sector) should include the procedures that would, according to point to management .

Therefore, as a whole, risk management at the national level is still primarily done on a sect oral basis, with the high-level government agencies in charge of given areas assuming a lead role for risk management in those. The analysis shows the influence of international and regional institutions in promoting and influencing the adoption of national risk management frameworks in specific sectors.

Line ministries and public agencies often have their own risk plans and officers in charge of managing sect oral risk. Such agencies include those in charge of customs and tax administration, budgeting and public debt management, border security and control, and other regulatory agencies in the fields of environment, urban planning, infrastructure, science and technology, food safety and quality, electric safety and energy production, public healthcare systems and medical waste management, among others.

Turkey, for instance, addresses economic and financial risk through the recently well-known Risk Analysis Units (2012) under the Directory of Risk Management and Control in its Ministry of Commerce. Risk Management is also part of the Strategy Formation Directorate in the Ministry of Finance. Turkey has a separate National Disaster and Risk Management Office under the Presidency. The adoption of risk management frameworks in national public administration in specific sectors is influenced by international law and normative guidance produced by international institutions. For instance, the work of the Basel Committee has spurred the adoption of prudential regulation frameworks at the national level in most countries.55 The European Union requires national risk assessments in order for member states to qualify for certain types of funds.56 The Sendai Framework for Disaster Risk Reduction and the Financial Action Taskforce (FATF) play similar roles in disaster and anti-money laundering. For instance, most countries in the sample were found to have anti-money

laundering and counterterrorism financing national risk assessments, based on FATF recommendations.

REFERENCES

1. Belan, Ľ., & Mišík, J. (2016). Manažérstvo bezpečnostného rizika, Žilina: Žilinská
2. univerzita v Žiline, 134.
3. Ministry of Defense of the Slovak Republic. (2017). Directive of the Ministry of Defense of the Slovak Republic no. 7/2017 on risk management in the field of financial management, Bratislava: Author.
4. Morong, S. (2012). Limity obranných zdrojov Slovenskej republiky a kolektívna bezpečnosť, Bezpečné Slovensko a Európska únia : zborník príspevkov zo 6. medzinárodnej vedeckej konferencie, Košice: Vysoká škola bezpečnostného manažérstva v Košiciach, 318-327.
5. Oláh, M., & Šidelský, Ľ. (2014). Riadenie rizika a úloha kontroly ako nástroja pre ich riešenie vo verejnej správe, Verejná správa a regionálny rozvoj, roč.10, č.1, 7-16.
6. Oláh, M., & Šidelský, Ľ. (2017). Predpoklady na väčšie zainteresovanie manažmentu pri riešení riadenia rizík vo verejnej správe, Scientific Journal Public Administration and regional developement, Vol. 13, Issue 1, 53-65.
7. Petrufová, M. (2014). Problems of manager competencies and teaching management in the military, Revista Academiei Forţelor Terestre, Vol. 19, Issue 2, 194-201.
8. Smejkal, V., & Rais, K. (2003). Řízení rizik, Praha: Grada Publishing, 272.
9. The National Council of the Slovak Republic. (2015). The Act No. 357/2015 Coll. on Financial Control and Audit. Bratislava.
10. Domokos, L. Risk analysis and risk management in the public sector and in public auditing, Public Finance Quarterly, 2015, 60: 1, 7-28. 3 Berg, H-P., 2010, Risk Management: Procedures, Methods, and Experiences, RT&A, 2 (17), June: 79-95.
11. Farahmand, F. 2005, A Management perspective on risk of security threats to information systems, Information Technology and Management, , 6: 2-3, 203- 225.
12. Barrientos, A., 2010, The labor market and economic risk: 'friend' or 'foe'?, Applied Economics, 35:10, 1209-1217.
13. Investorab. Financial Risks. 2018. Available at https://www.investorab.com/ investors-media/risks-and-risk-management/financial-risks/
14. Alter, R., 2019, contribution to the World Public Sector Report.
15. Rice, C., A.B. Zegart, Political risk: how businesses and organizations can anticipate global insecurity. New York: Twelve: 2018. 9 ISO 31000: 2018 Risk management guidelines available at https://www.iso. org/standard/65694.html
16. COSO ERM (Enterprise Risk Management). Integrating with strategy and performance. Available at https://www.coso.org/Documents/2017-COSOERM-Integrating-with-Strategy-and-Performance-Executive-Summary. pdf.
17. Saylor Academy, 2012, Risk Management for Enterprises and Individuals. Available online at https://resources.saylor.org/wwwresources/archived/site/textbooks/Risk%20Management%20for%20Enterprises%20and%20Individuals.pdf