European Research Studies Journal
Volume XXVII, Issue 1, 2024

pp. 142-153

Risk Management and Organizational Resistance to Threats

Submitted 15/01/24, 1st revision 12/02/24, 2nd revision 22/02/24, accepted 08/03/24

Zbigniew Ciekanowski[1], Marek Gruchelski[2], Julia Nowicka[3], Małgorzata Zdunek[4], Sławomir Żurawski[5]

Abstract:

Purpose: *The purpose of this article is to identify contemporary threats to organizations and determine their impact on organizational resilience. The publication addresses risk management and organizational resilience issues.*
Design/Methodology/Approach: *The authors pointed out global threats to contemporary organizations and characterized risk management in the organization. They then conducted a detailed analysis of statistical data, both national and European Union statistics, regarding the use of information technology in enterprises. The impact of individual threats on their functioning was also analyzed. The following research problem was formulated: What impact do individual threats have on organizational resilience, and how can proper risk management help in combating them? For the purposes of the research, the method of literature analysis, internet sources, and a detailed analysis of data from national and foreign sources, mainly the Central Statistical Office and Eurostat, were used.*
Findings: *Well-designed and implemented risk management can significantly increase the organization's resilience to threats. Thanks to it, the organization is better prepared to predict and identify threats, assess risk, take appropriate remedial actions, quickly respond to crisis events, and rebuild operations after a crisis event, allowing for increased resilience and opportunities for survival and development in an unstable environment.*
Practical implications: *The article discusses basic concepts related to risk management and organizational resilience and presents examples of actions that organizations can implement to increase their resilience to threats.*
Originality/Value: *In this article, the authors continue the discussion on risk management and organizational resilience, pointing out the need for research in the area of the impact of risk management on the organization's resilience to threats of various characteristics and the impact of risk management on various aspects of organizational functioning, such as financial results, reputation, or continuity of operation.*

[1]*Akademia Bialska im. Jana Pawła II w Białej Podlaskiej, Poland,*
ORCID: 0000-0002-0549-894X, zbigniew@ciekanowski.pl;
[2]*Warsaw Management University, Poland, ORCID: 0000-0003-4177-1613,*
gruchelscy@tlen.pl;
[3]*War Studies University, Poland, ORCID: 0000-0002-0778-0519,*
j.nowicka@akademia.mil.pl;
[4]*Poland, ORCID: 0009-0001-9305-2840, malgosia.piechowicz@gmail.com;*
[5]*State Academy of Applied Sciences in Chełm, Poland,*
ORCID: 0000-0001-9527-3391, slawomir.zurawski@onet.pl;

Keywords: *Resilience, organization, threats, risk management.*

JEL: *M14, L15.*

Paper type: *Research article.*

1. Introduction

In the contemporary world, wherein organizations must confront an escalating number and diversity of threats, effective risk management has become a crucial factor in ensuring their resilience. Organizational resilience is the capability to survive and continue operations in the face of threats. It can be achieved through actions that minimize the risk of adverse events and mitigate their negative consequences.

Risk management is a process that encompasses the identification, assessment, and management of risks to which an organization is exposed. It also involves taking preventive and corrective actions to reduce the likelihood of undesirable events and limit their adverse effects.

Enhancing organizational resilience to threats can be achieved through effective risk management. Organizations that have implemented effective risk management processes are better prepared to deal with potential threats. This article will discuss fundamental concepts related to risk management and organizational resilience, along with examples of actions that organizations can undertake to enhance their resilience to threats.

2. Threats to the Organization

Contemporary crises, induced by threats, originate from both macroeconomic and global conditions over which organizations often have no direct control. However, their occurrence significantly impacts organizational functioning (Ciekanowski, 2023). The environment in which organizations operate is characterized by an increase in novelty, speed, and intensity of changes, as well as complexity (Pluta, 2015; Spilbergs *et al.,* 2023).

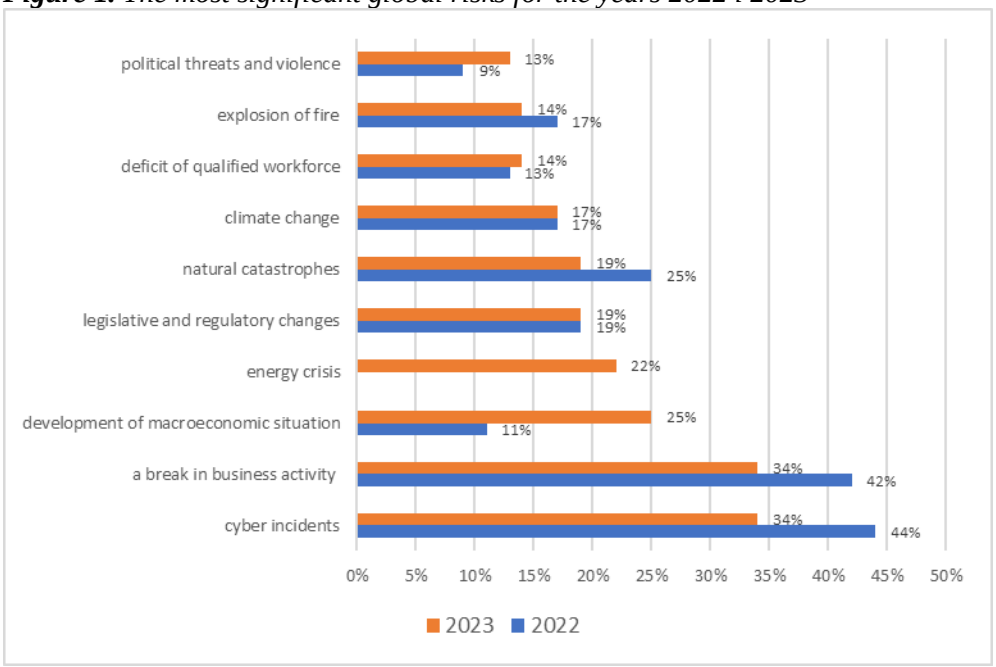
The primary threats that organizations have been grappling with for years include business disruptions, cyberattacks, natural disasters, and legislative and market changes. According to the Allianz Risk Barometer 2023 report, the most critical global risks for the year 2023 are as follows:

- Cyber incidents.
- Business interruption.

- Macro-economic developments.
- Energy crisis.
- Legislative and regulatory changes.
- Natural disasters.
- Climate change.
- Shortage of skilled workforce.
- Fire outbreak.
- Political threats and violence (Allianz Risk Barometer 2023).

Figure 1 presents a comparison of the most prevalent risks in 2022 and 2023.

Figure 1. *The most significant global risks for the years 2022 i 2023*



Source: *Allianz Risk Barometer 2023.*

As emerges from the analysis of the above data, cyber incidents represent the most significant threat to organizations, as they can lead to data loss, operational disruptions, and even monetary theft. To counter cyber attacks, organizations should implement appropriate security measures such as firewalls, antivirus and anti-spam software, as well as regularly train employees in IT security.

Additionally, the macroeconomic environment's development can also have a significant impact on organizational activities, especially in cases of inflation growth, rising energy costs, or economic downturns. The response to these and other threats lies in effective risk management. Organizations should regularly identify

and assess the risks they face. Subsequently, they should develop appropriate strategies and procedures to minimize risk.

3. Risk Management within the Organization

Risk management currently constitutes one of the most crucial areas of organizational functioning because it is closely linked to strategy and the pursued objectives. A modern organization, which takes on new challenges and thus undergoes a process of continuous development and improvement, must assess and manage risk (Wojtyto, 2019: Grima *et al.*, 2020; 2023; Thalassinos *et al.*, 2023).

Risk management in a business context can be defined as a process aimed at "identifying potential events affecting the company's operations and taking actions directed towards achieving its objectives" (Kuziak, 2011). Risk is an inherent element of organizational functioning, which either brings losses or gains, thus effective risk management should lead to the elimination or minimization of threats (Wojtyto, 2019; Velinov *et al.*, 2023).

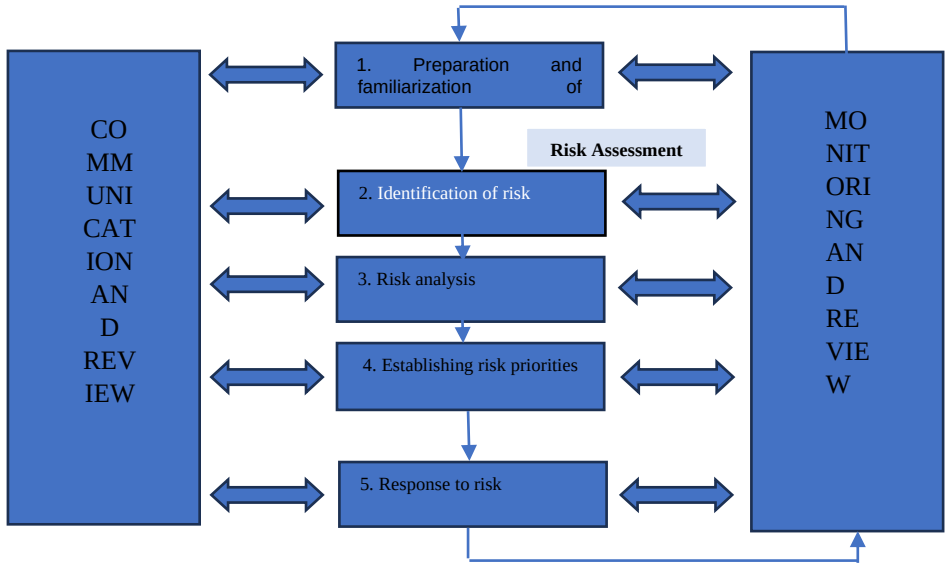
Taking the above into consideration, the stages of the organizational risk management process can be distinguished (Szczepańska, 2015):

- Identification, involving the determination of the area in which risk will be considered and the consideration of all threats to which the enterprise is exposed.
- Measurement, which quantitatively determines the level of risk in identified areas.
- Control, involving decision-making regarding specific action strategies using criteria such as risk size, risk sensitivity, and limitations or opportunities associated with risk.
- Monitoring and verification of the correctness of adopted solutions, e.g., risk estimation procedures (Risk Management in Organizations - How to Understand It?).

In order to effectively manage risk, it is necessary first of all to rely on the analysis of current statistical data. Therefore, it is necessary to constantly monitor the environment and one's organization and take appropriate actions that will lead to the risk reaching a minimum level. Its complete elimination seems impossible to achieve due to the multitude of factors influencing its occurrence (Risk management in the enterprise, 2023). Below is a diagram of the risk management process in the organization (Figure 2).

The ISO 31000 Risk Management - Principles and Guidelines norm provides support for organizations wishing to implement, within their management systems, a systematic, structured risk management process (Risk Management - Principles and Guidelines, 2023).

Figure 2. *Risk Management Process*



Source: *Own elaboration based on norm 31000.*

According to this norm, good risk management practices within a company are characterized by processes that:

- Create and protect organizational value.
- Are part of all processes within the structures of the organization.
- Form part of the decision-making process.
- Describe the nature of risk issues within the organization — their character and ways to deal with adversities.
- Are organized.
- Their mechanisms are based on current information.
- Are tailored to the nature of the organization's activities.
- Take into account human and cultural factors.
- Are transparent and comprehensive.
- Are dynamic, iterative, and allow for quick responses to any changes (e.g., regulatory).
- Facilitate the development of the organization, thus representing the opposite of the lack of a risk management process (Risk Management. Advice and Recommendations, 2023).

The Organization, to achieve success, must manage risk, but it should not fight against it. Managing it is one of the main areas aimed at increasing the efficiency of managing a given organization, which should be utilized to minimize threats or, in extreme cases, mitigate potential problems that will become key factors in development and functioning (Kraev, 2019).

Risk management is a continuous process that should be adapted to changing environmental conditions. Organizations should regularly conduct risk analyses to ensure that they are adequately prepared for the occurrence of risk. Risk management is an essential element of organizational management, which allows for:

- Protection against losses – risk management enables the organization to minimize the risk of events that may cause financial, asset, or reputational losses.
- Achieving objectives – risk management enables the organization to minimize the risk of events that may prevent it from achieving its objectives.
- Improving operational efficiency – risk management can help the organization identify and eliminate inefficiencies.
- Increasing competitiveness - organizations that effectively manage risk are more resilient to changes and better prepared for competition.

Risk management in an organization is not only about identifying problems and implementing preventive methods. It is very important how individuals participating in this process approach the implementation of the tasks assigned to them (4 methods for identifying risk in the enterprise, 2023).

Risk management should be a continuous process. Organizations should regularly conduct risk analyses to ensure that they are adequately prepared for the occurrence of threats, but also to collect and analyze data in order to effectively assess risk.

4. Resilience of the Organization

For several decades, it is not industry, but technological development that has changed reality so much that some researchers speak of the so-called civilizational revolution (Ciekanowski, 2019). Organizations are increasingly aware of the significance of emerging threats, yet a decisive majority still are not conscious of their potential impact on their operations, including security.

Resilience is an essential attribute enabling the sustainability of an organization and balancing its development. A resilient organization leads to an increase in value and relatively easily returns to a state of equilibrium (Zabłocka-Kluczka, 2012).

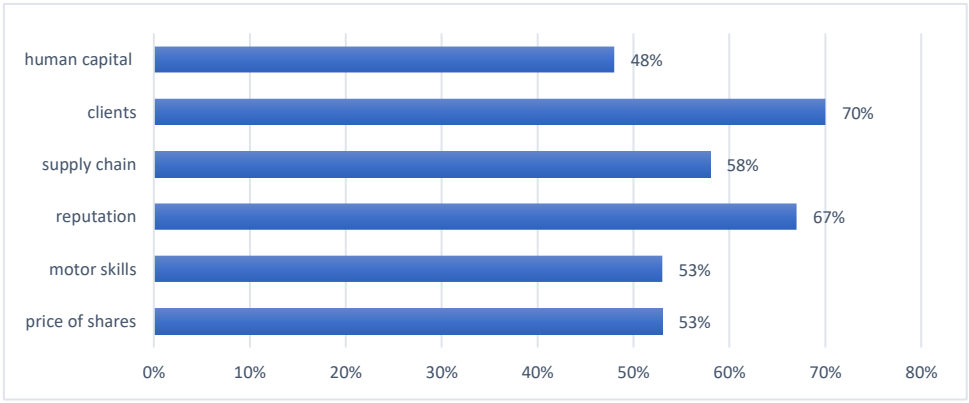
Resilience, in direct translation, means resistance, flexibility, elasticity, resilience, endurance, the ability to regenerate strength. Resilience is not just a single concept, but a broader concept of how businesses function. The most significant component of resilience is resilience itself, which T. Bishop and F. Hydoski defined as the ability of a company to return to its pre-stress state (Bishop, 2010). Four interrelated elements can ensure the resilience of an organization:

- Risk assessment – it is necessary to identify, categorize, and assess risk factors and indicate what strategy should be applied to limit them.
- Risk prevention – appropriate preventive strategies must be implemented to anticipate and counteract specific types of risk.
- Detection of irregularities according to previously adopted risk areas – e.g., through periodic audits or constant monitoring.
- Response to irregularities – scenarios of action in the event of irregularities should be prepared to minimize their negative impact on the enterprise (Majchrzak, 2020).

Analyzing current and emerging threats, it must be acknowledged that organizations must be resilient. More than ever, resilience is crucial for an organization's ability to compete and achieve strategic growth, as well as for its smooth operation (Risk Resilience Report. Keys to Building a More Resilient Business: Anticipation, Forecasting, and Agility, 2021).

Below are selected areas associated with risks directly impacting the resilience of every organization. The first threat is cyber threats. Figure 3 illustrates the impact of cyber threats on specific areas of the organization.

Figure 3. *Influence of cyber attacks on particular areas of the organization*



Source: *Risk Resilience Report. Keys to Building a More Resilient Business: Anticipation, Forecasting, and Agility, Marsch, 2021.*

Cyber threats are ubiquitous and intensifying, annually imposing significant losses and costs on organizations, posing risks in nearly every aspect of organizational functioning. The greatest impact of cyber threats occurs in the realm of data and information.

Cyber attacks can lead to data loss, data corruption, or unauthorized access to data. Unauthorized access to data may allow cybercriminals to steal personal, financial, or confidential data, which can have serious consequences for customers, employees, and the entire organization.

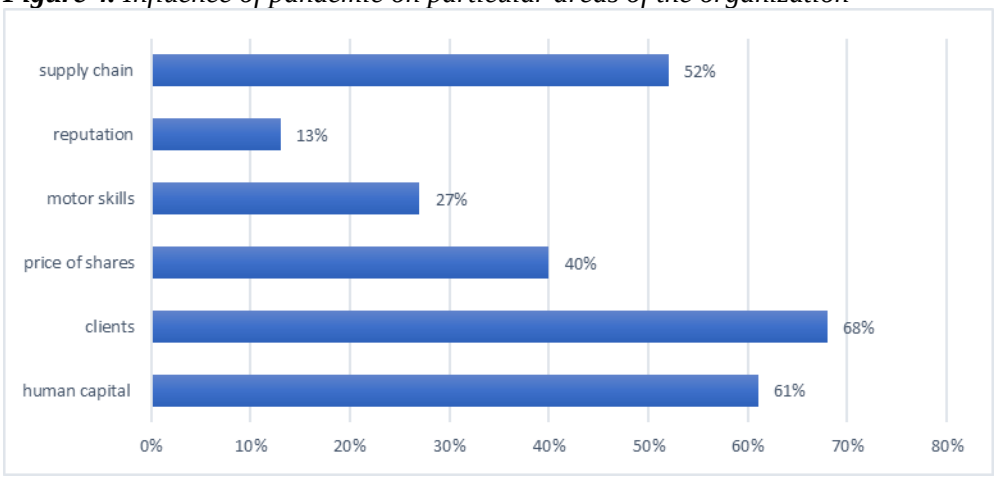
Of course, the specific impact of cyber threats on individual areas of an organization will depend on various factors, including the type of cyber attack, the resources and IT infrastructure of the company, and the industry in which it operates.

Another threat to organizational functioning and resilience was the COVID-19 pandemic, which had a significant impact on the operations and resilience of organizations worldwide. Among the main threats they had to face were:

- Health threats to employees. The pandemic caused an increase in illnesses and deaths among employees, leading to sick leave and staffing shortages.
- Financial threats. The pandemic resulted in decreased demand for products and services, leading to declines in sales and profits.
- Operational threats. The pandemic necessitated the implementation of new procedures and regulations, which could lead to disruptions in operational activities.

The impact of the pandemic on organizational functioning varied depending on the industry, size, and location. Organizations operating in industries particularly affected by the pandemic, such as tourism, hospitality, or catering, suffered the most. Below, in Figure 4, the impact of the pandemic on individual areas of organizations is illustrated.

Figure 4. *Influence of pandemic on particular areas of the organization*



Source: *Risk Resilience Report. Keys to Building a More Resilient Business: Anticipation, Forecasting, and Agility, Marsch, 2021.*

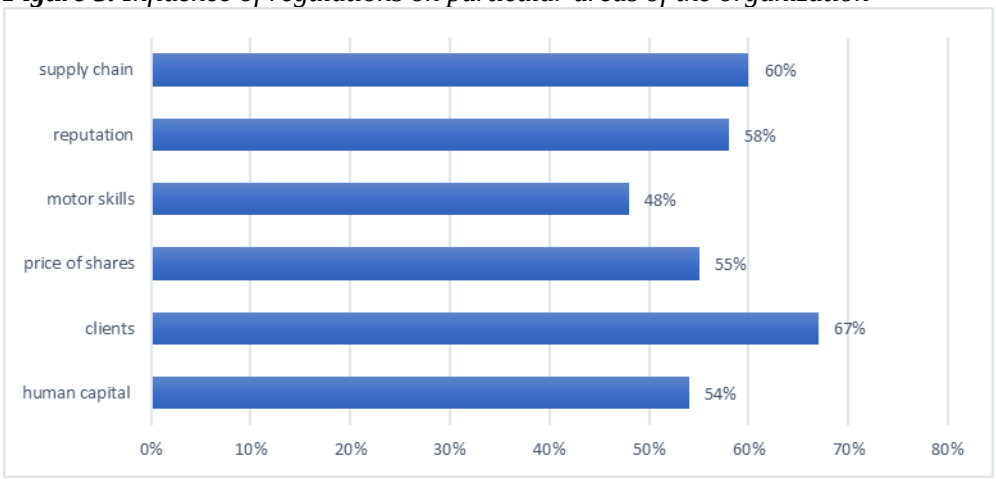
In order to minimize the impact of the pandemic on their functioning, organizations should undertake the following actions:

- Implement sanitary safety measures. Organizations could implement sanitary safety measures, such as masks, social distancing, and employee testing, to reduce the risk of illness.
- Introduce flexible forms of work. Organizations could introduce flexible forms of work, such as remote or hybrid work, to ensure employee safety and limit the risk of virus spread.
- Modify strategies. Organizations could modify strategies to adapt to new market conditions.

The COVID-19 pandemic has shown that organizations must be prepared for various types of threats, including those of a global nature. To increase their resilience, organizations should implement appropriate risk management and business continuity strategies.

The regulatory environment is constantly changing, especially for organizations operating in multiple countries. From tax regulations to data privacy regulations, environmental standards, labor issues, and more - compliance with regulations is complex and entails many other risks. Figure 5 illustrates the impact of regulations on various areas of the organization.

Figure 5. *Influence of regulations on particular areas of the organization*



Source: *Risk Resilience Report. Keys to Building a More Resilient Business: Anticipation, Forecasting, and Agility, Marsch, 2021.*

The greatest impact of regulations occurs in the area of data and information, particularly concerning clients. Regulations regarding personal data protection, information security, and privacy significantly affect how organizations process and protect data. Regulations can also have a significant impact on the financial and operational areas. Regulations concerning accounting, taxes, and consumer protection can affect operating costs and how organizations offer their products and services.

Various regulations can also affect the human resources area. Employment regulations, workplace safety and hygiene, and employee rights protection can influence how organizations hire and manage employees.

Of course, the specific impact of regulations on individual areas of an organization will depend on many factors, including the type of regulations, the industry in which the organization operates, and its size and location.

To minimize the impact of regulations on their functioning, organizations must take appropriate actions because regulations are part of the functioning of every organization. It should be noted that the effective functioning of organizations depends on knowing and complying with applicable regulations.

5. Conclusions

In today's world, in which organizations are exposed to an increasingly wide range of threats, risk management is an essential element of management and a key process for any organization, regardless of its size or industry. It enables the identification, assessment, and mitigation of threats that may disrupt the organization's operations or cause losses.

Well-designed and implemented risk management can significantly increase an organization's resilience to threats. Through it, the organization is better prepared to anticipate and identify threats, assess risk, and take appropriate remedial actions, respond quickly to crisis events, rebuild operations after a crisis event, thus increasing its resilience and chances of survival and growth in an unstable environment.

For risk management to be effective, it should be:

- based on a systematic approach, encompassing all areas of the organization's activities,
- conducted continuously, adapted to changing conditions,
- supported by the management team and all employees of the organization.

In further steps, it is worth examining the impact of risk management on the organization's resilience to threats of various characteristics. It is also worth examining the impact of risk management on various aspects of the organization's functioning, such as financial results, reputation, or operational continuity.

References:

Bishop, T., Hydoski, F. 2010. Odporność korporacji. Zarządzanie ryzykiem nadużyć i korupcji. Wydawnictwo Studio Emka, Warszawa.

Ciekanowski, Z., Czech, A., Nowicka, J., Zdunek M., Żurawski, S. 2023. Crisis Management and Crisis Situation in the Organization. European Research Studies Journal,Volume 26, Issue 4.

Ciekanowski, Z., Dawidziuk, R., Nowicka, J. 2019. Generacyjne wyzwania w zakresie funkcjonowania współczesnych organizacji. Nowoczesne Systemy Zarządzania, Zeszyt 14, nr 1.

Grima, S., Thalassinos, E.I., Cristea, M., Kadlubek, M., Maditinos, D., Peiseniece, L. (Eds.). 2023. Digital Transformation, Strategic Resilience, Cyber Security and Risk Management. Emerald Group Publishing.

Grima, S., Spiteri, J.V., Thalassinos, E.I. 2020. Risk Management Models and Theories. Frontiers in Applied Mathematics and Statistics, 6, 8.

Kraev, V.M., Tikhonov, A.I. 2019. Risk Management in Human Resource Management. TEM Journal, Issue 4.

Kuziak, K. 2011. Pomiar ryzyka przedsiębiorstwa. Modele pomiaru i ich ryzyko. Uniwersytet Ekonomiczny, Wrocław.

Majchrzak, M. 2020. Odporność przedsiębiorstwa czasach nadzwyczajnych zagrożeń. Adaptacja koncepcji resilience. Kwartalnik Nauk o Przedsiębiorstwie, 1/2020.

Pluta, A. 2015. Organizacja działająca pod presją czasu – szanse i zagrożenia. Studia i Prace WNEiZ US, nr 39/4.

Spilbergs, A., Norena-Chavez, D., Thalassinos, E.I., Noja, G.G., Cristea, M. 2023. Challenges to Credit Risk Management in the Context of Growing Macroeconomic Instability in the Baltic States Caused by COVID-19. In Digital Transformation, Strategic Resilience, Cyber Security and Risk Management (pp. 83-104). Emerald Publishing Limited.

Szczepańska, K. 2015. Zarządzanie jakością. Koncepcje, metody, techniki, narzędzia. Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa.

Thalassinos, E.I., Kadłubek, M., Norena-Chavez, D. 2023. Theoretical Essence of Organisational Resilience in Management. In Digital Transformation, Strategic Resilience, Cyber Security and Risk Management (pp. 133-145). Emerald Publishing Limited.

Velinov, E., Kadłubek, M., Thalassinos, E.I., Grima, S., Maditinos, D. 2023. Digital Transformation and Data Governance: Top Management Teams Perspectives. In Digital Transformation, Strategic Resilience, Cyber Security and Risk Management (Vol. 111, pp. 147-158). Emerald Publishing Limited.

Wojtyto, D. 2019. Metodyka zarządzania ryzykiem w organizacji. Organizacja i Zarządzanie, 12/2019.

Zabłocka-Kluczka, A. 2012. Odporność organizacji na kryzys. In: G. Bełz, S. Cyfert, eds, Strategie i mechanizmy odnowy przedsiębiorstw. Prace Naukowe, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław.

Netography:

Allianz Risk Barometer 2023. https://commercial.allianz.com/news-and-insights/news/allianz-risk-barometer-2023-press.html.

ISO 31000 Zarządzanie ryzykiem – zasady i wytyczne. https://www.iso.org.pl/uslugi-zarzadzania/wdrazanie-systemow/zarzadzanie-ryzykiem/iso-31000/.

ISO 31000 Risk Management. Porady i zalecenia. https://medium.com/blog-transparent-data/iso-31000-risk-management-porady-i-zalecenia-1427da84d24a.

Risk Resilience Report. Keys to Building a More Resilient Business: Anticipation, Forecasting, and Agility. https://www.marshmclennan.com/insights/publications/2021/june/risk-resilience-report.html.

Zarządzanie ryzykiem w organizacji – jak je zrozumieć? https://www.qualitywise.pl/zarzadzanie-ryzykiem-w-organizacji-jak-je-zrozumiec/.

Zarządzanie ryzykiem w przedsiębiorstwie. https://erif.pl/poradnik-przedsiebiorcy/zarzadzanie-ryzykiem-w-przedsiebiorstwie/.

4 metody na zidentyfikowanie ryzyka w przedsiębiorstwie. https://uhy-pl.com/blog-posts/4-metody-na-zidentyfikowanie-ryzyka-w-przedsiebiorstwie/.