RISKS AMPLIFIERS AT THE LEVEL OF ENTITIES IN THE FINANCIAL-BANKING SECTOR

Claudiu Ioan NEGREA[1]

Abstract: *Digitization has transformed the global economy, including by increasing productivity and expanding consumer access to information and new categories of goods and services. This digitization phenomenon has contributed to the development of many competitive markets that often crossed national borders.*

Considering that "economic development significantly depends on the complexity of the financial-banking system", the article deals with risk amplifiers regarding the entities in the financial-banking sector, given that digital technologies are present in all activities regarding this field.

In the modern financial landscape, the seamless delivery of financial services relies heavily on technology and interconnected data systems. This sector is entirely dependent on technology, although convenient for consumers, it exposes financial institutions to increased security risks, especially from cyber attackers who are increasingly sophisticated and present in a technology-driven world.

Thus, in a world in constant movement and development, we must pay special attention to risks, especially risk amplifiers that can turn a minor risk into a real major crisis if several vulnerabilities are not exploited simultaneously.

By adopting a comprehensive risk-based approach, financial institutions can make well-informed decisions related to the entity's resilience in line with investment objectives and offering attractive customer services.

Effective risk management ensures at the level of organizations a balance between risk mitigation and resource allocation, ensuring resilience and confidence in the financial system in an increasingly digitized world.

[1] Romanian Academy, "Costin C. Kiriţescu" National Institute of Economic Research, Bucharest, Romania, e-mail: claudiu.negrea@bnro.ro

This paper focuses on reviewing the amplifiers that can majorly destabilize the smooth functioning of an entity.

The events of recent years, the pandemic or the Russian-Ukrainian war, certify the need for a slightly different approach related to the major amplifiers that can create crisis situations.

This article proposes a risk-based approach to guide decision makers in identifying the optimal levels of security and recovery investments to protect their entity and ensure an optimal level of quality service.

The information in this paper can be used by any imported entity, in any field, to ensure an improvement in the level of risk management and a strengthening of operational resilience.

Keywords: *risks amplifiers, financial institutions, risks management*

JEL Classification: *O23; O42; P34; P42.*

Introduction

In the digitization era we can say that no recent innovation can be achieved without technology. This study attempts to answer the question... where is the place of man in a dynamic society dominated by technology?

The recent years reality reveals that digitization, in addition to the development facilities, speed and ease of use of new products and services, also brings a series of risks that, if they occur, can have serious consequences with a great impact on the well-being of the population.

Digitization has transformed the global economy, including by increasing productivity and expanding consumer access to information and new categories of goods and services. This digitization phenomenon has contributed to the development of many competitive markets that often crossed national borders.

Considering that "economic development significantly depends on the complexity of the financial-banking system", the article deals with risk

amplifiers concerning the entities in the financial-banking sector, given that digital technologies are present in all activities regarding this sector.

Risk management in any organization involves techniques for managing various internal and external risks, including operational risk, financial risk, business risk, legal risk, reputational risk, technological risk, etc. Some risks are more damaging to the health of an organization than others.

Regulations and technological developments are the main cause of digital transformation.

Lately, we can see that risk management is more and more difficult to manage considering the Covid pandemic or the war between Russia and Ukraine. All these elements could not be analyzed and taken into the risk calculation.

Literature review

The International Organization for Standardization in the standard ISO 31000:2018 - principles and generic guidelines on risk management, defines risk as the effect of uncertainty on objectives, and this definition must be viewed in compliance with the risk management mechanism that represents the set of coordinates management and control activities of an organization regarding risk management.

Risk management is constantly changing, and the concepts and models of risk management are significantly changing in the globalization context.

Regulations and technological developments are the main cause of this transformation.

To identify hazards within the organization and assess multiple risk factors, risk management is required. This is a "analyzing and assessing" method of the risks that are associated with the danger and possibility of an incident becoming a crisis as a result of amplifiers. Once identified, risks must be analyzed and managed accordingly.

The risk assessment must start from the entity's position and activities. Identifying threats is an ongoing process to take into account the evolution of amplifiers, at least those described in this research, record these hazards/threats and then analyze them (Bendel et al. 2021).

This process is important to be aware of the different types of risks and to identify the associated factors that are interdependent with factors such as employees, third party suppliers and customers or may be the general public. Risk awareness is necessary to mitigate crisis situations and is also beneficial for developing and testing effective business continuity plans. Periodic testing of control measures takes place to determine hazards and possible vulnerabilities at the level of the organization. In general, companies intend to apply hedging measures to mitigate negative situations. For financial risks this is a seamless process where organizations or individuals can easily eliminate the financial risks they are exposed to by using well-known financial instruments. But all these financial risk management mechanisms come with a cost that also reduces the return on investment.

The impact of risks can lead to the failure of some projects or even at the level of some organizations. When we refer to project risk management we can use a multitude of methods but the results of such an exercise must reveal the risk at the level of the organization, it includes the financial cost, the time for the successful implementation of the project, the business areas that will be affected of this new project and many other elements signified according to the project (Masuin et al, 2020).

Planning for unexpected situations can reduce the negative effect on the organization. In this case, there are also assumptions of unrealistic information or environment. Managers must link the market environment to associated risks, to external factors that may affect the organization. This process is difficult for the organization, although this process has played a key role for organizations since the beginning of risk management processes.

To increase business sustainability, hazard management must be provided by the same specialists and using the same tools used for risk management at the entity level (Venter, 2020). On the other hand, it is also difficult to measure the actual risks associated with different investments. Organizations can consider the same type of projects, which are completed in the past, so that these entities can easily identify the associated risks (Liu and Wang, 2019). After identifying the new risk categories, the entities must make a change to the risk management framework in line with the new identified risk categories and allocate additional resources for their effective management, or they can apply risk transfer measures by outsourcing, by concluding of insurance policies for certain risk categories.

Hedging strategies are mainly applied to reduce the risk of the organization through a perfect asset allocation or a certain risk transfer structure. The optimal hedging process is associated with changing investment opportunities. Investing in less risky funds or stocks can reduce investment risks (Kočenda and Moravcová, 2019). On the other hand, the return on less risky investments is low. Consequently, managers should consider less risky funds with high value returns. This is quite difficult for the risk manager, although it is necessary for organizations (Buehler et al. 2019).

The risk management framework is also associated with the necessary changes within the organization. This process not only identifies changes but also uncovers business opportunity. Different types of knowledge are needed to determine the requirements of strategic change. Communication skills are important to change the management of a company. Effective communication helps clarify the changes that are actually needed, and the changes will be made with the requirements.

Good communication saves time for people involved in the process and increases the chances of a perfect implementation. Active listening also plays a key role in establishing a good communication process within the company. The main purpose of making a plan in a business procedure requires adequate management of orientational and structural changes.

Employees participate in actively listening to various instructions given by management. Every organization has no clue about change management and the requirement of understanding the organizational capability process remains unknown to them. Change management focuses on improving the alignment of the various procurement procedures within the management of the strategic process. The core process includes the proper alignment of project requirements necessary to manage change and achieve project objectives. The present leadership within a company plays a key role in maintaining the generation of strategic thinking based on the purchase of change within the employees.

To get a real understanding of the risk management framework and the impact of policies and coverage, many journals and articles are considered. Most of the articles are focused on how a company or individual can better manage their risks. On the other hand, it is also necessary to identify the causes of the risks.

This article fully considers these factors to make a brave choice. Articles suggest how a company can mitigate adverse situations; on the other hand, this paper also focuses on how organizations reduce the causes of risk.

Methodology

The qualitative research methodology used in this study involves a comprehensive review and analysis of the relevant literature and legislation relating to the risk and resilience of financial institutions. The research methodology integrates theoretical and practical studies and analyzes to ensure a high level of understanding of risk assessment and management mechanisms, with an emphasis on the factors that can amplify these risks.

Information for this research was collected through a systematic review of academic articles, research papers, industry reports, regulatory documents and legislative frameworks relevant to the research area. Online databases, academic journals and authoritative sources in the field

of risk management were consulted to ensure the inclusion of the most recent and reliable information. The collected data were subjected to rigorous qualitative analysis techniques, including thematic analysis and content analysis. The aim was to identify recurring themes, patterns and insights related to risk assessment, vulnerability identification, risk mitigation, operational resilience, interdependence risks and the integration of entity security and resilience measures.

Based on the literature and legislation review, we have developed a list of the most important categories of amplifiers that can significantly affect an entity to guide any entity in the process of improving its risk management framework.

This framework aims to address the challenges entities face in ensuring an optimal level of operational resilience.

The qualitative approach was chosen due to its ability to provide a deep understanding of complex phenomena, allowing to explore and gain insights into the challenges and good practices associated with the risk management. Qualitative research allows for a nuanced examination of different risk factors, vulnerabilities and potential impacts on the entity, allowing for a more holistic view of an entity's resilience.

Further research is needed to develop decision-making models that can determine the ideal level of investment in risk reduction strategies and streamline investments in ensuring optimal resilience.

Such models must consider the specific vulnerabilities of each entity, consider generalized approaches to optimal investments, and consider at least the types of amplifiers presented in this paper.

In order for risk management to be as effective as possible, risk analysis models are needed that are easy to use, that can identify vulnerabilities both at the level of the entity and at the level of the sector in which it operates.

Results and discussions

Unfortunately, even at this point we cannot say that the risks management, especially operational ones, is a well-known process and the operational resistance of financial entities can be ensured in extreme but plausible conditions.

The two situations in the last period that affected the continuity of activity at the level of many entities highlighted an extremely positive aspect for the process of ensuring the continuity of activity, namely the increased capacity of entities to adapt to new types of threats.

The complexity of a risk analysis is also given by the analysis of risk amplifiers that can transform an ordinary incident into a crisis situation.

An effective risk analysis must also evaluate a series of factors that can amplify the effects in the event that the risks materialize. Among these factors, the most relevant ones from my point of view are:

• The difficulty, sometimes even the impossibility of entities to have complete and detailed information related to the developments that must be brought to the services offered in order to preserve their competitive advantages and to maintain consumer satisfaction in parallel with maintaining an optimal level of security of these services, especially in the context of digitization;

• The limited time for substantiating and adopting strategic decisions, especially in the management of crisis situations;

• Forecast and its uncertainties; Starting from Taleb's statement which emphasizes that most of the time forecast errors are major, a fact also highlighted by Friedman in 1953 who said that "the only relevant test of the validity of a hypothesis is the comparison of its predictions with experience"[2] makes risk management to be an extremely difficult process. The lack of specialists and financial resources make the activity of risk forecasting an extremely complex one in which, in addition to the

[2] "The only relevant test of the validity of a hypothesis is comparison of prediction with experience". Milton Friedman 1953;

evaluation of usual threats, the possibility of totally unforeseen situations must also be evaluated, which most of the time have a major impact on an entity.

• The actions of major economic powers can negatively affect the proper functioning of national economies and local entities; Most of the time, the largest national entities, especially those in the financial field, are multinational companies, and an uncompetitive or abusive approach can destabilize the national economy and affect the well-being, comfort and health of the population.

• Frictions between nations are a permanent risk generating factor, from wars, terrorism, to cyber attacks, all of which can lead to the manifestation of the risks at the entity level. The most recent situations certify an exponential increase in cyber attacks as a result of the war between Russia and Ukraine, whose targets were mostly the authorities of the member states that had reactions condemning the military actions in Ukraine. Even Romania was the victim of such attacks that led to the unavailability of the internet pages of some authorities, and following investigations it was found that these attacks were orchestrated from the territory of Russia.

• Concentration risk, dependence on external suppliers is one of the most important factors that can generate risks at the level of national critical infrastructures. The largest technology providers are often companies outside the country, and dependencies on the technologies provided by them are crucial in the context of digitization. A serious operational incident at the level of such a provider could generate major effects worldwide, given the extent of the spread of these services. In these cases we have to think about the SWIFT interbank communication network, Visa, Mastercard payment schemes, technology providers Microsoft, Oracle, IMB, etc. In the case of these entities, local authorities do not have the power of supervision and control and most states do not have the necessary mechanisms to ensure a substitution of these services so that the effects of an operational incident at the level of these companies do not affect national consumers.

This risk of concentration is also present at the level of financial market infrastructures which at that point are irreplaceable and a major operational incident at their level would have major effects that would lead to the blocking of the local financial market or in the case of a financial market infrastructure that provides services cross-border could generate systemic risk at the level of the region.

An example of this could be the Target platform and the services it offers (TARGET2, TARGET2-Securities and TIPS[3]) used at European level for the settlement of payment obligations in euros. A blockage at the of this infrastructure level would generate a blockage in the settlement of payments in euros at the European level with systemic effects concerning the European financial system and the European economy. And in the event that the incident would have greater effects than one day, the impact would exceed the borders of Europe, generating an impact on all financial entities at the global level that ensure the settlement of payment obligations or receipts in euros through the TARGET platform.

• The industry's reliance on legacy technologies whose security protocols no longer respond to new categories of cyber threats and the number of people who can provide support for these programming languages is in major decline. Legacy technologies limit the ability of financial entities to keep all IT systems in use up to date, as these updates can lead to bottlenecks in the exchange of information between the different types of applications that are deployed in the infrastructure.

• A new risk of concentration is generated by cloud[4] service providers who concentrate a large number of entities, especially in the financial field and e-commerce platforms, and whose good functioning is fully dependent on the availability of cloud services. A potential incident at

[3] TARGET Instant Payment Settlement – the instant euro payment system operated by the ECB.

[4] Use of cloud services - the technical infrastructure that an entity uses is located outside the entity's premises in a data center that is maintained by the cloud computing service provider in order to benefit from increased computing power and access . to new technical and functional facilities.

the level of these cloud infrastructures would have a major impact on all entities that use these services for their current activities.

• Digitization and innovation, especially in the financial services sector, present an opportunity for the development and implementation of new technologies and services, while increasing operational resilience. But these new technologies also come with a number of vulnerabilities, not identified in the implementation phase, that can be exploited by cyber attackers.

• New types of service providers, especially payment service providers are, in particular, technology-based companies that enter the financial market and offer their customers new services mainly based on technology, completely digitizing the relationship between the consumer of financial services and the provider of these services (fintech companies[5]). Usually these companies do not know the risk management mechanisms involved in the provision of complex financial services and what are the compliance requirements established by the legislation in the financial field. Many times, these companies cause losses among consumers due to poor risk management and exclusive reliance on technology, which makes these companies totally vulnerable to cyber attacks. The lack of physical infrastructure at the branch level makes it almost impossible for consumers to access their own funds in the event of a major operational incident that leads to the unavailability of the technical infrastructure.

• Disinformation campaigns or "fake news" are increasingly targeting financial entities. These campaigns are spread through social media, often succeeding in creating panic situations among consumers of financial services. According to an analysis[6] published by the World Economic Forum, more than two-thirds of respondents estimated a major increase in the risks associated with the spread of false

[5] FinTech (Financial Technology) known today as "financial technology", describes a business that aims to provide financial services by using software solutions and other advanced technologies.

[6] The Global Risks Report 2019 14th Edition pg. 12 https://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

information. For financial services, where transactions take place in a split-second, disinformation campaigns represent a significant threat that can have effects of manipulating financial markets. An example of such an attack was that in January 2019[7] on BlackRock, when a few days before the official publication of the annual letter of BlackRock CEO Larry Finck, it was forged and distributed through various electronic media through which it was a major change in the company's investment profile was announced. This false information was also picked up by major news agencies Financial Times, Cnbc.com, etc.

This incident was generated to protest the investment activity of the company and not for the purpose of financial gain and demonstrates the ease with which disinformation campaigns can be made to generate crisis situations.

Social networks and the use of bot farms make these disinformation campaigns extremely complex and easy to provoke and the speed of propagation of these messages is very high and most of the time they manage to penetrate quickly into the consciousness of consumers creating situations of panic among them.

Financial markets are particularly susceptible to manipulation based on disinformation, as these markets are often driven by the perception of fear, and the resulting speculation presents opportunities for actors involved in disinformation campaigns and can benefit them by moving the markets in such a way as to deliver them with getting rich quick.

Another similar case is the May 2019 incident at England's Metro Bank, where the bank's share price was found to have fallen by at least 9 percent after false rumors circulated on WhatsApp and Twitter that the bank was close to bankruptcy and that customers should empty their accounts as soon as possible so as not to lose their money in the accounts opened at this institution.[8]

---

[7] https://news.wiztopic.com/news/the-blackrock-case-trusting-corporate-and-financial-information-a-new-challenge-for-financial-companies-and-media-e145-7e09e.html

[8] https://www.businessinsider.com/whatsapp-rumour-started-run-on-metro-bank-2019-5?r=US&IR=T

Such an attack could be beneficial to the actors who orchestrated this dissemination of false information and in most cases generate negative movements in the market where the shares of the companies against which such manipulation generated campaigns are traded. In the previously highlighted case, the possibility of short-term profit can be seen considering that this campaign led to a considerable drop in the credit institution's shares.

These disinformation campaigns can have systemic effects if they target a state or strong government authorities (central banks, ministries, large state-owned companies, etc.) generating investor distrust in such an economy and undermining the economic and financial soundness of that country.

• While the cloud technology paradigm is a pressing issue today, we must also consider quantum computing power (quantum computers) and the ability of these computers to crack the encryption keys used by the financial system today. Quantum computing can provide exponential improvements in the increase of processing power, the calculations required in the transaction process and for the identification of fraud attempts, but the implementation of these new technological solutions requires a laborious process of development and operationalization and, at the same time, extremely expensive.

• Hackers for hire represent another threat to the financial system, and the situations where the victims of these attackers are financial entities that are constantly increasing. Malicious actors, more often than not, do not directly compromise the targeted entities, but use the services of these cybercrime groups. There is a wide range of services offered by these cybercrime groups, from developing disinformation campaigns to launching complex attacks to compromise or disable critical consumer services.

Conclusion

This study reveals that risk management is essential for any type of organization or individual. Companies face a variety of risks, including economic, financial and operational risks. Entities continuously develop

their risk management mechanisms and continuously improve their control and risk mitigation measures.

Situations of uncertainty increase risks at the level of any organization. Right at the time of writing this material we can say that the situation of uncertainty is more and more present considering the developments in the financial markets and the uncertainties related to the war on the borders of our country.

Thus, the analysis of the amplifiers presented in this material will provide an additional level of awareness of potential external threats that can affect an organization.

Today, on the market there are a number of risk transfer mechanisms or their coverage through various financial instruments or guarantee policies, but all of them have no value in the event of the materialization of a major risk at the entity level that can generate a significant reputational risk and with the potential to close the entity's activity.

In conclusion, I believe that the most effective risk management process is specialized staff in risk management and ensuring the necessary resources to provide and maintain the entity's risk tolerance level and the availability of activity at the entity level.

No risk management measure is complete, the risk management process is a dynamic and complex one that must be permanently anchored to economic and social realities.

People are the basic element in every organization!

References

Buehler, H., Gonon, L., Teichmann, J. and Wood, B., 2019. Deep hedging. Quantitative Finance, 19(8), pp.1271-1291;

"Bussinessinsider.com., 2019, A false rumor on WhatsApp started a run on a London bank, link available at:

https://www.businessinsider.com/whatsapp-rumour-started-run-on-metro-bank-2019-5?r=US&IR=T.";

Friedman, M., 1953. The only relevant test of the validity of a hypothesis is comparison of prediction with experience;

Kočenda, E. and Moravcová, M., 2019. Exchange rate movements, hedging and volatility spillovers on new EU forex markets. Journal of International Financial Markets, Institutions and Money, 58, pp.42-64;

Liu, Z. and Wang, J., 2019. Supply chain network equilibrium with strategic financial hedging using futures. European Journal of Operational Research, 272(3), pp.962-978;

Masuin, R., Latief, Y. and Zagloel, T.Y., 2020. Development of integration risk on integrated management system in order to increase organisational performance of construction company. International Journal of Project Organisation and Management, 12(2), pp.164-177;

Schwenk, B., Madsen J. T. and Fekete, M., 2021. Applying DEFCON and the Homeland Security Advisory System in organisational risk management. SCENTIA International Economic Review, 1(1), pp.192-202;

The Global Risks Report 2019,14th Edition pp.12, World Economic Forum, link available at: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf;

Venter, C., 2020, A Reflection on SSM to Improve Organisational Risk-Based Project Governance and Decision Support Mechanism, ECRM 2020 20th European Conference on Research Methodology for Business and Management Studies: ECRM 2020, Academic Conferences and publishing limited, pp. 300;

Wiztopic.com., 2019, The BlackRock case: Trusting corporate and financial information, a new challenge for financial companies and media, link available at: https://www.wiztopic.com/news/the-blackrock-case-trusting-corporate-and-financial-information-a-

new-challenge-for-financial-companies-and-media-e145-7e09e.html;

Zhen, X., Vinnem, J.E., Yang, X. and Huang, Y., 2020, Quantitative risk modelling in the offshore petroleum industry: integration of human and organizational factors. Ships and Offshore Structures, 15(1), pp.1-18.