FINANCIAL CONTROL: DEVELOPMENT PERSPECTIVES IN THE CONTEXT OF DIGITALIZATION

Nicoleta Cristache [1*], Valentina Butmalai [2], Alina-Florentina Saracu[3], Irina Susanu[4]
[1)2)3)4)] "Dunarea de Jos" University in Galati, Romania

Abstract

The article analyses financial regulation, emphasising its importance in guaranteeing financial security and stimulating sustainable economic growth. It discusses the challenges that economies face in the information age, the factors influencing these processes and the emerging risks that may arise in this constantly changing landscape. In addition, the threats and risks targeting financial security in the digital age are identified and presented in detail, and the relevant indicators for their assessment are carefully analysed. The article also highlights the importance of new practices for verifying and monitoring financial processes. A crucial point of the research is that, for insurance purposes, the effective development and strengthening of various forms of public control, it is essential to invest in improving the financial cultivation of the population and in promoting a more solid economic culture that supports adaptation to the new challenges of the digital economy.

Keywords: financial control, financial security, public control, financial management, identity verification, digitalization, cyber fraud

JEL Classification: G18, G28, G32, O33, D53, I38, D83

Introduction

In the age of digitalization, humanity has put new digital technologies at its service, developed neural networks, uses digital platforms, applies multifunctional programs, and a "smart home" helps in everyday life, with services - special programs, including "Ghișeu.ro". All this greatly simplifies, accelerates the process of obtaining information, services, opens access to transactions, and improves communications. However, along with progressive forms of interaction between people, digitalization also entails risks.

[*] Corresponding author, **Cristache Nicoleta** – cristache.nicoleta@yahoo.de

First of all, this is the improvement of cyber fraud technologies. Psychological tricks are actively used to mislead, deceive, confuse and manipulate.
The article analyses how digitalization influences financial control activity, highlighting both opportunities and emerging risks. Namely, it aims to assess the impact of new technologies on financial control, as well as identify the challenges related to cyber fraud and behavioural traps, fraudster techniques and recommended behavioural responses to counter the traps. The resources needed for sustainable monitoring were explored, and a risk-oriented preventive control algorithm for data protection was proposed.
The structure of the article is organised, starting with an introduction to the topic and continuing with the literature review and research methodology. This is followed by the results and discussion section of the research, and the conclusions summarise the key ideas and emphasise the importance of a proactive and integrated approach.

1. Review of the scientific literature

Professional literature highlights the direction of development of financial supervision in the digital era and highlights the role of innovative technologies and new economic models in strengthening financial security. Dancikov and Omelchenko (2019) emphasise the need for continuous monitoring to manage economic risks, in particular by integrating advanced financial solutions. In the same context, Omelchenko (2019, 2020) studied various methods of preventing financial threats, with a particular focus on identifying and preventing fraud schemes. The authors highlight the importance of adopting a proactive approach based on continuous risk assessment to detect potential fraud early and take appropriate preventive measures before it affects financial stability. Meanwhile, Mnatsakanyan and Kharin (2020) discuss how digitalization affects business management, and Glubokaya (2022) explores emerging trends in green finance, which are increasingly integrated into financial control strategies. Dovbiy and Kovrizhkina (2022) discuss the integration of corporate social responsibility (ESG), and Gorevaya and Aksenova (2019) emphasise the adaptability of management systems in the face of digital transformations. This research demonstrates how digitalization is redefining the financial control process, requiring innovative strategies to address new challenges and protect the integrity of the financial system.

2. Research methodology

The research methodology will focus on analysing the impact of digitalization on financial control and financial security, considering emerging risks and ways to prevent them. The research will include a review of relevant literature to identify current trends and innovative practices in financial control. The literature review is selected based on its relevance to the topic of digital transformation and financial control, focusing on recent and impactful studies available through open access platforms.
The analysis will include qualitative data from the observation and interpretation of existing laws to assess the effects of digitalization on public financial control and on the economic culture of the population. This research will analyse the relevant legislative

framework for the areas of control and digitalization in Romania, focusing on three main sectors: public procurement, labour protection and environmental protection. This methodological approach will allow for the integrated development of applicable legislation, as well as the related institutional and digital monitoring and control mechanisms.

3. Results and discussion

The main purpose of the research was to investigate and analyse the economic sectors with the greatest growth potential, to identify the most effective ways in which financial controls can evolve and adapt, in order to achieve the highest standards of financial security. Research objectives:

• analysis of risks and threats, as well as identification of indicators that influence financial security;

• establishing the role and importance of control in combating threats to economic and financial security, both at the international level and at the national and industrial level, for legal and natural persons.

• characterization of approaches to ensuring security in the era of digitalization;

• to reveal resources to ensure sustainable monitoring and timely response to threats to economic security through public control, improvement of economic culture and financial literacy;

• to analyze behavioral traps, fraudster techniques and recommend behavioral responses to counter the traps;

• to present a preventive and risk-oriented control algorithm as an effective way to protect data in the digital space.

Only properly organised, well-established, timely updated and indicator-responsive control can preserve the benefits of digitalization, resist abuse and capitalise on the overconfidence of technology users.

Currently, control has a diverse range of methods and techniques, which allow addressing the complexity of current economic challenges. The diversity of control strategies and organisational mechanisms makes it possible to anticipate, prevent and effectively combat the negative effects generated by economic changes, thus ensuring stability and sustainability in the face of them. Among these effects is the manipulation of knowledge related to the perception and reaction to information, essential for the decision-making process. So, there are two systems of perception of reality: 1) subconscious; 2) conscious. In 90% of cases, we use the first system to guide us to action. We do not think about where to start brushing our teeth, how to get out of bed, take a shower, get into the car, go to the nearest store or on the way to the office where we have been going for many years. All such and similar actions are performed automatically, as if at a subconscious level. And only to solve truly complex, important or for the first time (without experience in solving problems) do we use the conscious system.

So, scammers often use this property of the psyche. They disguise complex problems as seemingly similar everyday situations to force a decision to be made on a subconscious

level, by analogy with another completely unrelated task. Thus, they impose solutions that are inappropriate to the situation.

Other behavioural traps can also be used - the perception of loss is more painful for a person than receiving a benefit. It leads to unnecessary expenses and the imposition of unnecessary expensive services, etc. In order to correctly perceive the situation, it is recommended not to make hasty decisions. "Counting to 10" is a rule that allows you to switch from the first system to the second. In complex and expensive situations, it is recommended to contact experts and listen to different reasoned points of view before making a decision. The more important the task, the more detailed the study is needed. In practice, we often carefully consider trivial decisions (how to spend an evening, a trip, a visit, New Year's Eve, etc.) and solve complex and expensive problems without additional work. So, without a lack of experience and proper training, we entrust the purchase of an apartment to a representative of the developer, trust the manager to buy a car or a phone, make investments in business, and believe in advertising. There are many such tricks in everyday life. To save nerves and money, one should switch to the second system more often. The more complex the problem, the more thorough the analysis and the more balanced the decision should be. In general, the following methods of protection can be distinguished:

• if there is not enough experience in decision-making, it is better to contact an expert;

• not all internet sources must be trusted, but only verified (proven, professional) ones;

Loss must be calculated. Establishing a personal limit, upon reaching which participation in the transaction will cease under any circumstances;

• when making important decisions, it is necessary to take breaks to switch the brain to the second system.

Digitalization certainly contributes to systematization, awareness, algorithmization, reducing information processing times, and forming databases.

Digital platforms have simplified purchases, trading, the education system, healthcare, and obtaining government services etc.

Cybercriminals have also become more active, and new opportunities have opened up for them. It is enough to create a malicious link, launch a virus, solicit personal information about a customer over the phone or obtain it using a phishing site, after which such information is often used to obtain a loan, withdraw money from a card, commit securities, property and investment fraud.

Only the user themselves can protect the interests of bona fide participants in business processes, being vigilant and informed, and if we are talking about the interests of companies, organisations, industries or the state, then counteracting any kind of fraud is made with the help of financial control. The organisation of state, departmental and internal financial control is defined in the legislation. In order to ensure digital security, Romania and the National Bank of Romania have implemented essential measures to ensure digital security, protecting critical infrastructures and personal and financial data of citizens. An example is Law no. 362/2018 on cybersecurity, which regulates the protection of essential infrastructures, such as telecommunications networks and financial systems, obliging operators to report security incidents. Also, by complying

with European regulations, such as GDPR, they allowed Romania to increase the protection of personal data, and banks were forced to adopt strict measures to prevent abuse. These regulations and measures are fundamental to creating a secure digital environment, having a direct impact on reducing the risks of cyber attacks and fraud. Cyber fraud is dangerous not only for individuals and legal entities, but it can also cause damage to the state. It can be used for terrorist financing, money laundering, triggering military conflicts and establishing a world order against the will of the people. One of the effective ways to implement security measures that work to prevent threats is to monitor them. For the purpose of monitoring the AML (Anti-Money Laundering)/CFT (Countering the Financing of Terrorism) risks carried out by credit institutions, the following risks are distinguished: country, customer, commercial transaction and credit institution involvement.

A prosperous economy requires the presence of financial security, which, in turn, cannot be guaranteed without financial control (Figure no. 1).

Figure no. 1: Control as an element of economic prosperity

Source: developed by the authors

As Figure no. 1 indicates, economic well-being can only be achieved if financial security is strengthened and effective financial control is in place In the absence of adequate control and regulatory measures, the phenomenon of capital flight, economic crime and corruption risks redirecting national resources, which could otherwise be allocated to solving urgent social problems, instead of contributing to the development of the economy and the well-being of society. For progressive economic growth, strict control over budget replenishment and expenditure patterns is necessary. Financial control is designed to monitor the availability of resources, productivity, efficiency, rationality and profitability of resource use. It is aimed at ensuring optimisation and obtaining the best results based on available resources and minimum investments.

In the context of financial control, a number of internal threats negatively influence economic stability and the efficiency of public institutions. Among them is the increase in economic crime, manifested by the intensification of crimes such as tax evasion, fraud and money laundering, which affect the public budget and undermine trust in

authorities. In parallel, the increase in corruption contributes to the distortion of the decision-making process and the inefficient use of resources, affecting good governance.

Another phenomenon with a major impact is capital flight abroad, through which funds are transferred outside the country in response to economic instability, lack of trust in fiscal policies or the desire to avoid domestic regulations. This weakens the investment capacity of the national economy. At the same time, a decrease in real incomes of the population is observed, often caused by rising prices and stagnant wages, which reduces domestic consumption and worsens social imbalances.

All these elements can be amplified in the context of a financial crisis, characterised by instability in financial markets, lack of liquidity and institutional collapse. In addition, rising inflation reduces the purchasing power of citizens and creates additional pressures on budgetary and fiscal control policies.

In addition to internal risks, financial control is also exposed to external threats, which can significantly affect the economic stability of a state. One of these is the loss of external economic positions, reflected in the decrease in competitiveness in international markets, the reduction of foreign direct investment or the loss of access to global financial resources. This phenomenon limits the country's economic capacity to attract capital and modern technologies.

Another major threat is the lack of involvement in international financial structures, which means poor integration into global networks of regulation, supervision and financial collaboration. This isolation affects transparency, information exchange and the ability to react to transnational threats.

Also, the risks related to espionage in the financial and credit sector are increasingly relevant. These include activities of illegal collection of sensitive information about the state's financial infrastructure, banking policies or capital flows, with the aim of undermining economic stability or providing a strategic advantage to external actors.

Last but not least, there is the phenomenon of intentional criminalisation of economic activities, a practice whereby certain sectors or initiatives are deliberately targeted through restrictive regulations or abusive interpretations, with the aim of discrediting, controlling or eliminating them from the market. These actions may stem from external pressures or transnational economic interests and affect fair competition and economic sovereignty.

Financial security involves high-quality control over financial flows and an effective system for preventing financial abuse and fraud. The risks and dangers that threaten financial stability and security are presented in an illustrative manner in Figure no. 2, highlighting the various challenges and vulnerabilities that can affect the financial system and its protection.

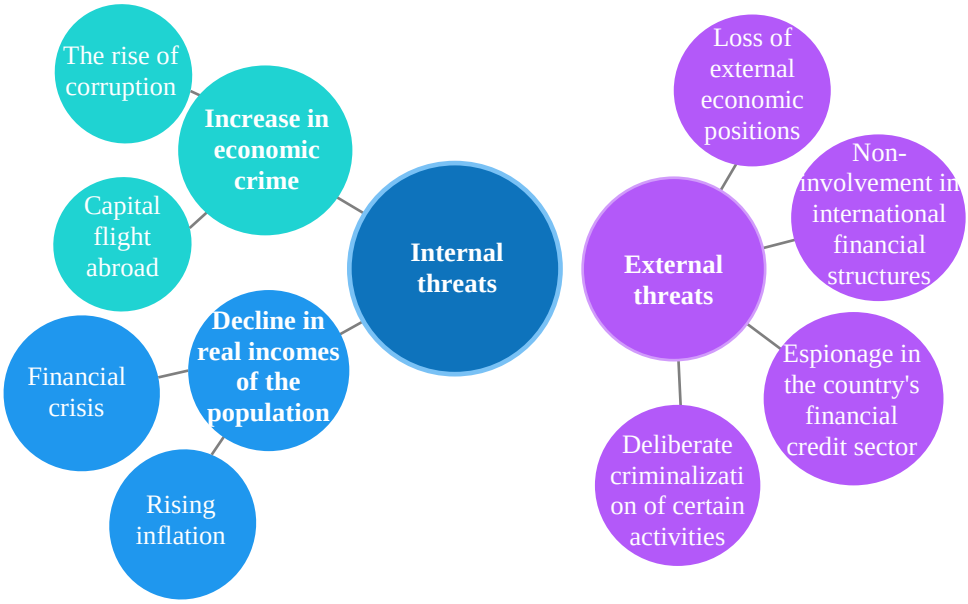

Figure no. 2: Financial security risks and threats

Source: developed by the authors

Specialists in the field have identified the following essential components of an effective financial security system:

- the budgetary and fiscal system;
- the banking system, including the money and foreign exchange market;
- the system of extra-budgetary funds.

Risk-oriented control allows for the protection of budget revenues, ensures the monitoring and identification of customers and their transactions, and creates conditions for the accumulation and fair distribution of funds among beneficiaries. For control purposes, financial security identifiers are used (Figure no. 3).

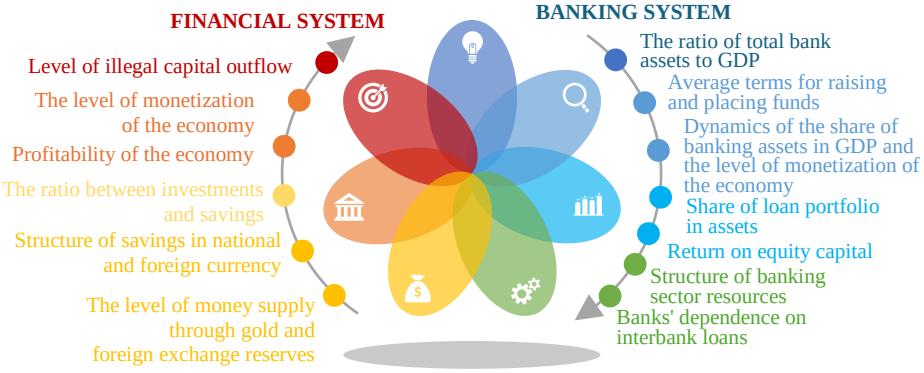

Figure no. 3: Financial security identifiers

Source: developed by the authors

Today, public control is of particular interest. It is provided for by the current legislation. However, from our point of view, its potential is not fully utilised. Public control is provided for:

• for the purpose of carrying out procurements (Law no. 98/2016 on public procurement in Romania) — to track procurements, there is the SEAP website, the national platform that centralises and facilitates the public procurement process in Romania;

• in the field of labour protection (Law no. 319/2006 on safety and health at work, European Directive 89/391/EEC on the introduction of measures to encourage improvements in the safety and health of workers at work, Law no. 53/2003 - Labor Code). These regulations are implemented and monitored through close collaboration between trade unions, government agencies, competent labour inspectorates and authorised employee representatives;

• in the field of environmental protection (Law no. 265/2006 on environmental protection, Law no. 107/1996 on waters, European Directive 2008/98/EC on waste, Law no. 53/2000 on the protection of wild fauna and flora, etc.) - carried out by public authorities, by citizens in the role of public inspector (voluntary, free of charge), public associations and NGOs.

Public control is carried out in the following forms:

• public monitoring;
• public inspection;
• public examination;
• public discussion;
• public hearings.

Public control refers to the agencies and entities responsible for monitoring and supervising the activities of state agencies, local government agencies, national and municipal public organisations and other entities exercising public authority, by national legislation. This activity includes not only public inspections, but also detailed analysis and critical assessment of documents issued and decisions taken by competent

authorities. In order to ensure the efficiency and transparency of public control, a high level of financial education and a solid economic culture are at the heart of this process, both within the relevant institutions and among those responsible for its implementation and supervision. Only in such a context can a correct and responsible management of public resources be guaranteed, thus ensuring efficiency in the use of funds and in making economic decisions.

Conclusions

It has been found that financial security is the pillar of a prosperous economy, and its assurance cannot be achieved and maintained without high-quality financial control, organised in a professional and efficient manner. In the current context of digital transformations, it is essential to develop a preventive control system, based on constant risk assessment, to anticipate and minimise emerging threats. It is also crucial to implement new forms of public control, adapted to modern technological challenges and opportunities, to ensure both the efficiency and transparency of regulatory and monitoring processes. In this direction, research indicates that cyber fraud represents a significant threat to the advantages of the ever-expanding digital economy. In order to protect economic systems and users from the negative impact of cyber fraud, it is imperative to identify and analyse existing risks, emerging fraud models, behavioural traps that may arise, as well as advanced technologies used in these illicit practices. In this regard, the recommended behavioral responses for the correct management of traps are examined, methods for monitoring and protecting data in the digital environment are presented, and the risk-oriented control organization for combating money laundering and terrorist financing (Anti-Money Laundering - AML/ Countering the Financing of Terrorism - CFT) within credit institutions is analyzed.

The originality of the article lies in the integrated approach to financial control in the context of digitalization, by correlating national and European legislation with new technologies and associated risks, such as cyber fraud. Among the limitations of the research is the lack of a quantitative analysis or applied case studies. For the future, it is recommended to expand the research by applying empirical methods (interviews, surveys, institutional case studies), but also by developing a framework for assessing the digital maturity of institutions involved in financial control.

References

[1] Dancikov E, Omelchenko E. ”Financial supervision as a tool for combating threats to economic security when implementing innovative financial technologies”. Law and digital economy. Issue 4, 2019 (06). pp. 5-9. DOI 10.1 7803/2618-8198.2019.06.4.005-009.

[2] Glubokaya I, ”Modern Trends in Green Finance”. 2022. Business and Economics: Practice and Theory. No. 4. pp. 11–15.

[3] Gorevaya E, Aksenova K. ”Modern management transformations in innovative companies”. Business. Education . Law . 2019. No. 2. pp. 109-116.

[4] Kovrizhkina L, Dovbiy I, ”Business Social Responsibility in the Era of ESG Transformation”. Management in modern systems. 2022. No. 2. pp. 20–32.

[5] Mnatsakanyan AG, Kharin AG. ”Cost approach to business management in the era of digitalization”. 2020. Intellect. Innovations. Investments. No. 5, pp. 72–82.
[6] Omelchenko E. ”Control and audit are measures to prevent threats and challenges to financial security”. Economics and management: problems, solutions. 2023. Vol. 2. No. 5(137). pp. 179-186. DOI 10.36871/ek.up. 2023.05.02.026.
[7] Omelchenko E. ”Identifying suspicious schemes as a way to prevent threats to financial security”. Audit. 2020, issue 5, pp. 5-7.
[8] Omelchenko Yu, ”A risk-based approach to assessing the quality of financial controls of a credit institution for AML/CFT purposes”. Audit. Issue 1, 2019, pp. 21-25.
[9] Petrova N, Ovechkina A, ”Digital transformation of the economy: Challenges and opportunities”. 2021. Bulletin of the Saint Petersburg University of Economics. No. 2 (128).
[10] Semenov A, Gubaidullina A. ”Digital transformation of company business models”. 2021. Construction economics. No. 2. pp. 49-55.
[11] Tsyganov S, Lebedeva T, ”Innovative development of companies in the digital age”. Intellectual resource management. Litres, 2021.
[12] Tiron-Tudor, A., Cordoș, G. S., & Mutiu, A. (2022). Digital transformation and auditors’ responsibility in fraud detection. Journal of Risk and Financial Management, 15(6), 247. https://doi.org/10.3390/jrfm15060247
[13] Van der Aalst, W. (2016). ”Process mining: Data science in action” (2nd ed.). Springer. https://doi.org/10.1007/978-3-662-49851-4
[14] Wang, J. (2023). ”Fraud detection in digital payment technologies using machine learning”. Journal of Economic Theory and Business Management, 1(2), 1–10. https://doi.org/10.5281/zenodo.10926495
[15] Zhou, W., & Kapoor, G. (2011). ”Detecting evolutionary financial statement fraud”. Decision Support Systems, 50(3), 570–575. https://doi.org/10.1016/j.dss.2010.08.007