Internal Control Tools to Strengthen the Fight Against Fraud in the European Union

Irina-Ștefana Cibotariu
„Stefan cel Mare" University of Suceava, Romania
irina.cibotariu@usm.ro

Abstract

This paper aims to systematically reconstruct and analyze both typical and atypical models of fraud schemes prevalent in various sectors and channels of the modern landscape. It seeks to explore and delineate the evolving tools and strategies developed to combat the spread of fraud. The primary focus is not to provide an exhaustive analysis of the entire scope of specialized literature on fraud, but rather to offer an insightful description of various forms of fraudulent behavior within a company context, highlighting their prevalence and consequences. This approach allows for a nuanced understanding of fraud dynamics, contributing significantly to the field of fraud detection and prevention.

Key words: audit, fraud, internal control tools, irregularity, European Union
J.E.L. classification: K40, K42, K49

1. Introduction

The concept of internal control varies significantly depending on the sector in which it is applied. In the public sector, internal control is predominantly about verification activities executed by entities external to the monitored body, yet operating within its framework. This approach is often guided by international best practices, such as the COSO (Committee of Sponsoring Organizations of the Treadway Commission) framework and relies heavily on national supervisors to integrate these practices into existing supervisory systems effectively. On the other hand, in the financial sector, the definition of internal control is more specialized due to unique business requirements. Here, an internal control system is designed not only to ensure compliance and operational efficiency but also to manage market risks adequately. This sector has seen a more explicit and rigorous application of internal control systems, driven by both regulatory demands and the inherent complexities of financial transactions. The scenario in the private sector, however, presents a stark contrast. Lacking a clear and universally accepted definition of internal control, many private organizations have yet to adopt a system tailored to their specific needs. In several cases, the very concept of 'control' is narrowly perceived as synonymous with audit or basic accounting functions, overlooking its broader strategic implications. This myopic view often results in missed opportunities for enhancing organizational efficiency and mitigating risks.

This lack of a comprehensive understanding and application of internal control mechanisms in the private sector is particularly concerning in the context of fraud prevention. Fraudulent activities within companies can take various forms, each with unique characteristics and impacts on the organization. Without a robust internal control system, these entities remain vulnerable to both internal and external fraud schemes, which can have far-reaching financial and reputational consequences. Therefore, this paper emphasizes the critical need for a nuanced approach to internal control across all sectors, particularly in the private sector. By exploring and analyzing diverse fraud schemes and the evolving tools to combat them, the paper aims to highlight the importance of bespoke internal control systems. These systems should not only comply with regulatory requirements but also be agile enough to adapt to the unique challenges and risks specific to each organization. This approach is pivotal in fortifying the fight against fraud, thereby contributing

significantly to the broader landscape of fraud detection and prevention in the European Union.

2. Theoretical background

Companies that have begun to engage with the concept of internal control often encounter the challenge of inadequate support in constructing a comprehensive system. This highlights the need for a deeper understanding of internal control as a dynamic process integral to an organization's operations.

1. The internal control system is not a static entity; it is a process interwoven with the core activities of planning, execution, and monitoring within a business (Conyon et al., 2016, p. 21). Its effectiveness is maximized when it becomes a part of the organization's culture, involving individuals at all hierarchical levels, not just those at the top. While it is crucial to understand that an internal control system provides reasonable assurance towards achieving objectives, it cannot offer absolute certainty due to inherent limitations like human error or intentional circumvention of controls.

Indeed, this system is at its most effective when it is integrated into the structure of an organisation and becomes part of its corporate culture. Moreover, it consists not only of manuals and documents, but also of people at all hierarchical levels of a company, not just at the top. This definition of an internal control system also specifies how management and the board of directors can expect from the control structure only reasonable, not absolute, assurance on the achievement of objectives; therefore, no matter how well an internal control system is structured and implemented, it will never guarantee total assurance, as it is in any case vitiated by the limitations inherent in any type of system, such as human failures. human omissions or avoidance of controls by one or more individuals.

2. As outlined in the 1992 CoSO report, the internal control system comprises five interrelated components, adaptable to organizations of varying sizes (DeZoort et al., 2018, p. 74). These components are:

The control environment, whose constituent factors are:

- Integrity and ethical values;
- The value of competence;
- The board of directors or audit committee;
- Management philosophy and style;
- Organisational structure;
- Allocation of skills and responsibilities;
- Human resources policies and practices.

Risk assessment, the elements of which are:

- General business objectives;
- Specific objectives for each activity;
- Risk analysis and assessment;
- Change management.

The current global context, marked by the COVID-19 pandemic and geopolitical tensions such as the war in Ukraine, necessitates the adaptation and enhancement of internal control systems. The European Commission is working to augment existing tools and develop new strategies to address the unique challenges presented by these circumstances, particularly in the management of EU funding. This adaptation includes recognizing and mitigating new risks, adapting control activities to remote or hybrid working environments, ensuring effective communication in a rapidly changing context, and continuous monitoring to respond to evolving threats and opportunities.

In conclusion, the theoretical underpinnings of internal control systems in the modern context underscore the importance of a flexible, comprehensive approach. This approach must be responsive to the changing landscape of risks and organizational dynamics, ensuring robust fraud prevention and efficient management in various sectors.

3. Research methodology

This research will adopt a mixed-methods approach to evaluate the effectiveness of ARACHNE, EDES, and other EU anti-fraud instruments. The methodology involves a comprehensive analysis of data from the European Commission, ECA, and CSES surveys to quantitatively assess the usage and impact of these tools across EU Member States. A comparative study will examine the implementation of national anti-fraud strategies, augmented by specific case studies of Member States with active tool usage. Interviews with EU officials and auditors, coupled with survey analysis on the best practices from the Anti-Fraud Knowledge Centre, will provide qualitative insights. Additionally, the research will review the legal and policy frameworks underpinning tools like EDES and assess the technological aspects of tools like GetI, evaluating their contribution to enhancing analytical capacities in fraud detection and prevention.

4. Findings

The Commission encourages the use of ARACHNE, an integrated IT tool for data mining and data enrichment. It has been developed by the Commission to support managing authorities in administrative controls and management verifications of the Structural Funds (European Social Fund and European Regional Development Fund). It has also been extended to European Agricultural Fund for Rural Development (EAFRD) projects and will be used for all agricultural funds following the CAP reform.

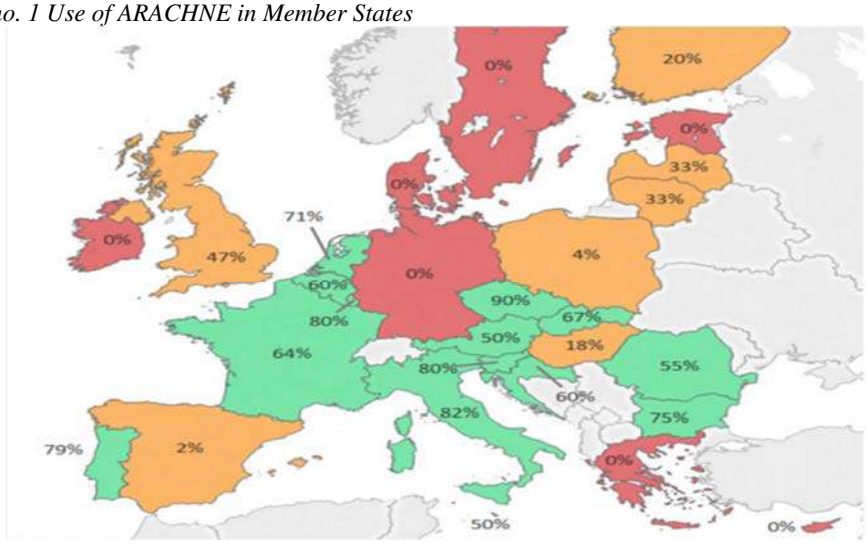
ARACHNE establishes a comprehensive database of EU projects implemented under the Funds, provided by managing authorities and paying agencies, and enriches this data with publicly available information to identify, based on a set of risk indicators, projects, beneficiaries, contracts and contractors. that may be susceptible to risks of fraud, conflict of interest and irregularities.

The tool provides extremely valuable risk alerts to enrich management checks, but provides no evidence of error, irregularity or fraud. ARACHNE can increase the efficiency of project selection, management checks and further strengthen fraud identification, prevention and detection.

In view of the risks that may arise, it is necessary and appropriate to make widespread and systematic use of tools such as ARACHNE which would allow the fight against fraud, irregularities, conflicts of interest and double funding to be stepped up.

Despite its merits, the extent to which Arachne is used by MAs varies. By September 2022, 21 Member States were using Arachne, of which 16 had integrated it into their management and verification processes for at least one operational program. According to Commission figures, Member States used Arachne for 165 operational programs in 2022, representing 54% of total EU cohesion policy funding for the period 2016-2022, excluding the European Territorial Cooperation Objective of the European Regional Development Fund. The use of ARACHNE can be seen in the following image.

Figure no. 1 Use of ARACHNE in Member States



Source: ECA, based on Commission figures

Despite its merits, the extent to which Arachne is used by MAs varies. By September 2022, 21 Member States were using Arachne, of which 16 had integrated it into their management and verification processes for at least one operational program. According to Commission figures, Member States used Arachne for 165 operational programs in 2022, representing 54% of total EU cohesion policy funding for the period 2016-2022, excluding the European Territorial Cooperation Objective of the European Regional Development Fund.

DG REGIO's Joint Audit Directorate for Cohesion Policy indicated that 56% coverage of operational programs for the 242 programs supported by DG EMPL and REGIO for the period 2016-2022 has been achieved by June 2021. Another study commissioned by DG REGIO found that the majority of MAs were not using Arachne (only one third of MAs were using Arachne as a risk assessment or fraud detection tool). Arachne is often used by authorities in combination with other IT tools, most commonly national IT tools and databases, but these have a narrower geographical scope. In countries where Arachne is not used, there are generally national and regional IT systems or other similar tools and databases offering similar functionalities. However, the majority of MAs using the tool considered that it added value.

The most active Arachne users seem to be Bulgaria, Czech Republic, France, Italy, Latvia, Romania and Slovakia.

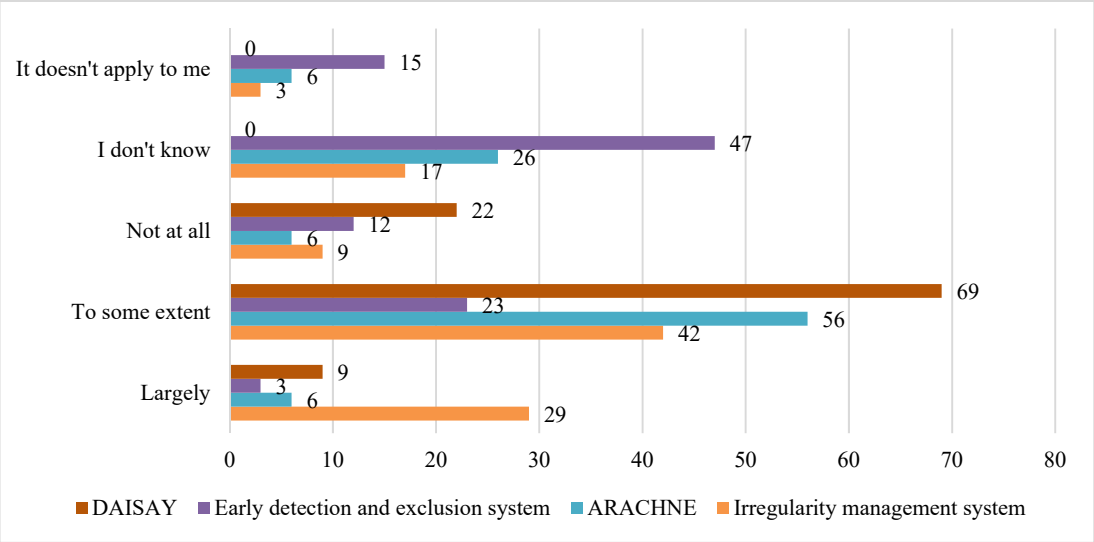
The Commission manages the Early Detection and Exclusion System (EDES). EDES is referred to in Articles 135-145 of the Financial Regulation applicable to the EU budget. It is an instrument to strengthen the protection of the EU's financial interests against unsafe entities and persons by excluding such economic operators from participating in procedures for the award of EU funds under direct and indirect management. Prohibited practices include a wide range of behaviours affecting professional integrity (e.g. fraud, corruption and serious professional misconduct) and poor performance (such as significant shortcomings in contract implementation). In particular, EDES allows:

- Early detection of entities or persons, which present a risk to the EU's financial interests;
- Exclusion of these economic operators from receiving EU funds under direct and indirect management and/or imposition of a financial penalty;
- Registration of the above information in the EDES database, which is accessible to the community of financial actors responsible for the implementation of Union funds;
- In the most serious cases of exclusion, publication of the names of the entities or persons concerned on the Commission's website.

EDES allows for a centralised assessment of exclusion situations while protecting the fundamental rights of the persons and entities concerned, in particular their right to be heard. The uniqueness and power of EDES lies in the power granted to EU institutions and bodies to act "in the absence of a final national decision or, where applicable, a final administrative decision". The

imposition of sanctions can be based on established "facts and findings" arising from audits, verifications or controls carried out under the responsibility of the authorising officer responsible, investigations by OLAF or non-final administrative decisions by national authorities or international organisations. The decision to impose a sanction on non-compliant economic operators can only be taken by the relevant authorising officer after first obtaining a formal recommendation from the centralised inter-institutional committee (European Commission).

Figure no. 2 The effectiveness of anti-fraud instruments developed by the EU

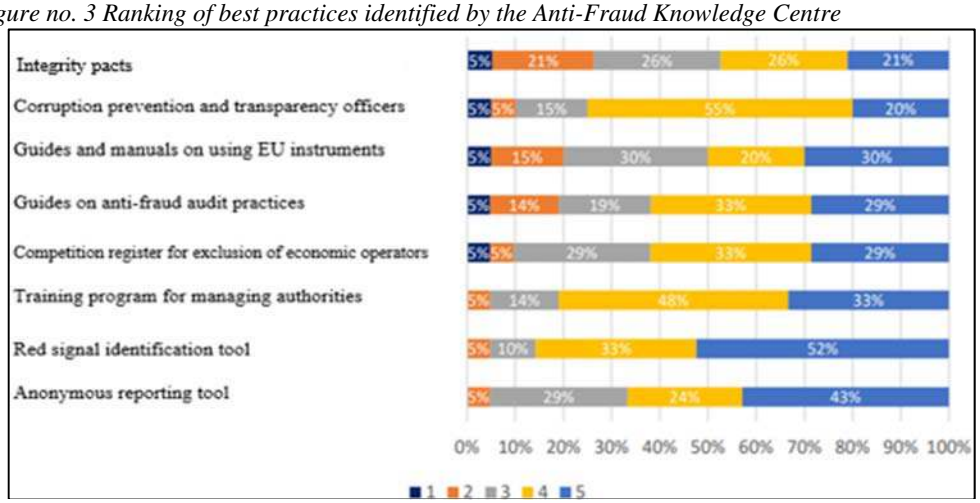


Source: CSES online survey

Among the initiatives OLAF supports is the Anti-Fraud Knowledge Centre. This online facility provides access to a wider range of material (a library, definitions and glossary, guidelines and legislation, etc.) and includes a best practice section.

The Commission's Anti-Fraud Knowledge Centre lists 37 best practices under a number of headings - whistleblowing systems, systems and tools, cooperation mechanisms, red flags, sanctions, training and guidance. In each case there is a brief description, an explanation of the key success factors and an indication of replicability elsewhere. Some good practices focus specifically on EU funds under shared management, while others have a wider role in tackling fraud in relation to public spending in general. We examine and add to the Anti-Fraud Knowledge Centre's good practices later in this section. In the survey for this study, we asked respondents to rank the various good practices identified by the European Commission's Anti-Fraud Knowledge Centre (this was done on a scale of 1 to 5, with 1 meaning that the practice is not useful for fraud prevention and 5 meaning that the practice is very useful). As can be seen in the graph below, whistleblowing systems, tools for identifying "red flags" and training programs ranked relatively well, although the situation is not clear (European Anti-Fraud Office).

Figure no. 3 Ranking of best practices identified by the Anti-Fraud Knowledge Centre



Source: CSES online survey

The GetI project aims to increase the analytical capacity of OLAF staff working on both operational and strategic tasks by improving the accessibility and visualisation of information, speed and flexibility in querying data. The diversity of data formats and the volume of unstructured data has in recent years generated a need for an environment, tools and functions that facilitate analytical work. Through a collection of open source and commercial software, GetI aims to automate many time-consuming tasks and implement modern technologies such as artificial intelligence.

National anti-fraud strategies

In 2021, EU Member States have communicated the development of more IT tools to strengthen the protection of the EU's financial interests, which will be of particular importance in addressing the challenges that have arisen with the war in Ukraine, the COVID-19 pandemic and new ways of managing EU funding.

Table no. 1 IT tools implemented by EU Member States in 2022

Member state	Instrument	Budget sector
Bulgaria	Use of a centralised electronic platform in public procurement	All expenditure
Czech Republic	Update procedures for verifying ownership structures and conflicts of interest	Cohesion policy
Denmark	Merging data to identify cases of double funding	Cohesion policy
Estonia	Launch of a cybercrime information and notification website	Horizontal
	Improving the Public Procurement Register	All expenditure
Germany	Self-assessment of fraud risk for ESF and ERDF federal programs	Cohesion policy
Hungary	Use of ARACHNE and EDES	Cohesion policy and the Most Deprived Fund
Lithuania	Purchase of analytical software and hardware for the implementation of anti-money laundering and counter-terrorist financing measures	Horizontal
	IT tools and regulatory measures	Agriculture
Netherlands	Enhanced digital grant application	Agriculture
	Risk assessment tool: selection of fraud-prone lotteries	Agriculture
Romania	Digitised checks by the competent bodies of the ESI to streamline public procurement controls	Cohesion policy
Spain	Direct access by AFCOS to Spanish social insurance databases	All expenditure
Sweden	Better procurement statistics	All expenditure

Source: www.eur-lex.europa.eu

5. Conclusions and recommendations

In conclusion we can say that fraud has always been the focus of attention of specialists and lawyers, it affects almost all areas of business from data breaches affecting end-customer privacy rights and payment security to ransomware attacks requiring large amounts of money from organisations. When not dealt with proactively, fraud can affect companies' financial results by pulling resources away from core activities and priorities, damaging brand reputation and wasting profits. In extreme cases, it can even cost lives. (Lederman, 2010, p.54)

After all of the above it can be seen that fraud prevention efforts have lagged behind with the incredible speed at which fraudsters have acted, fraudsters have been and still are a growing target.

Today, it is undeniable that the world we live in is going through a period of crisis and, as the media or various analysts or thinkers often point out, this is affecting various aspects of life. But a closer look at the situation in the light of all the above reveals a common denominator, a factor that lies, so to speak, at its source, namely that all crises cascade down from the one and only crisis, the crisis of values. The crisis of values does indeed lead to a loss of what are the cornerstones of an upright and ethical way of life based on the solid cornerstones of moral integrity.

There is an awareness that with the passage of time technological developments refine and improve the tools adopted by fraudsters to achieve their goal. At the same time, the evolution itself refines, on the one hand, the regulatory frameworks and, on the other hand, the prevention and detection best practices that entities adopt, with the necessary adaptations to the individual reality. Following a simple logical process, when a new fraudulent manoeuvre occurs, the bodies set up to reduce the risk of fraud study and implement tools designed to reduce the damage that occurs, with the ultimate aim of preventing it. (Reffett, et al., 2010, p. 15). Digital fraud technologies continue to evolve, even as financial institutions and businesses adopt the latest strategies to make digital payments more secure. The new generation of fraudsters is adapting quickly to innovative technologies. To prevent fraud, you should know your vulnerabilities and familiarise yourself with the right technologies to mitigate risks. As a final point, it should be noted that the most important investment an entity can make in avoiding the occurrence of fraud is prevention, which is essential to minimise risk exposure and reduce the risk of fraudulent acts committed by internal or external agents, and the real benefits will be known in the long term, as effective strategies will be developed to limit the occurrence of this phenomenon and consequently the associated economic losses.

6. References

- Conyon, M. J., & Lerong He., 2016. Executive Compensation and Corporate Fraud in China. *Journal of Business Ethics*, vol. 134, no. 4, p. 21. Available at: https://doi.org/10.1007/s10551-014-2390-6
- DeZoort, F. Todd, & Paul D. Harrison.2018. Understanding Auditors' Sense of Responsibility for Detecting Fraud Within Organizations. *Journal of Business Ethics*, vol. 149, no. 4, p. 74. Available at: https://doi.org/10.1007/s10551-016-3064-3
- EUR-Lex: Access to European Union Law. [online] Available at: https://www.eur-lex.europa.eu [Accessed 09.06.2023].
- European Anti-Fraud Office (OLAF), n.d. European Anti-Fraud Knowledge Centre. [online] Available at: https://antifraud-knowledge-centre.ec.europa.eu/index_en [Accessed 17.05.2023].
- European Commission, n.d. [online] Available at: http://ec.europa.eu/budget/edes/index_en.cfm [Accessed 07.06.2023].
- European Court of Auditors, 2019. [online] Available at: https://www.eca.europa.eu/lists/ecadocuments/sr19_06/sr_fraud_cohesion_en.pdf [Accessed 23.11.2023].
- Lederman, L., 2019. The fraud triangle and tax evasion. In *Proceedings. Annual Conference on Taxation and Minutes of the Annual Meeting of the National Tax Association* (Vol. 112, pp. 1-54). National Tax Association. Avaiable at: https://www.jstor.org/stable/27067393
- Reffett, A. B., 2010. Can Identifying and Investigating Fraud Risks Increase Auditors' Liability? *The Accounting Review,* vol. 85, no. 6, p. 15. Available at: https://doi.org/10.2308/accr.2010.85.6.2145