Social Economic Debates
Volume 14, Issue 1, 2025
ISSN 2360-1973; ISSN-L 2248-3837

FINANCIAL AND ACCOUNTING SECURITY AND CONTROL OF ENTITIES IN THE CONTEXT OF THE NECESSITY FOR DIGITALIZATION

PhD Student Ana-Rebeca NEAGU (ION),*
Affiliation: IOSUD-SDSE Valahia University of Târgoviște, România,
E-mail: rebecaneagu@yahoo.com

PhD Student Ștefan Alexandru PREDA,
Affiliation: IOSUD-SDSE Valahia University of Târgoviște, România,
E-mail: predastefanalexandru@yahoo.com

PhD Professor Florin RADU
Affiliation: IOSUD-SDSE Valahia University of Târgoviște, România,
E-mail: florin.radu@valahia.ro

Abstract: This study highlights vulnerabilities at the entity level, particularly regarding the evolution of fraudulent practices, with adverse effects on accounting. Considering the imperative of integrating digital technology into the current professional landscape of employees and the asymmetrical threats exposed during the COVID-19 pandemic, this study reveals critical aspects that demand careful consideration and tailored solutions. Technology has a double role, challenging and helping: some employees or managers can use it for negative purposes, vitiating the activity and performance of the entity, while others can prevent and remove such negative behaviors through the undeniable benefits brought by the digital tools. Following this study, several ways can be identified to improve the internal control process, to increase the degree of security of the entity from a financial-accounting point of view, to prevent, from an early stage, and to combat fraud already installed.

Keywords: economic fraud, digital tools, accounting, control, performance

JEL classification: D23, D73, M21, M41

Introduction

In a constantly changing and technologically evolving world, entities are prone to easily lose control over employees, which is why there is a need to adopt measures to raise awareness of the increased risk of developing fraudulent behaviour among them. The identified threats come both from inside (which are also the most difficult to detect) and from outside the entity, the security culture implemented by the manager of the organization / entity being able to blur the scourge that can generate vulnerabilities, but also to draw attention to areas with degenerative potential.

Social Economic Debates
Volume 14, Issue 1, 2025
ISSN 2360-1973; ISSN-L 2248-3837

The digital era gained momentum with the onset of the COVID-19 pandemic, at the point where, at the recommendation of the Organisation for Economic Co-operation and Development (OECD), tax administrations suspended or reduced audit activities for a while, in the context of the rapid multiplication of cases of disease, a decision that generated many discussions at taxpayers' level: thus, while some considered that the decision was based on a confident and cooperative attitude in the population during crisis situations, others considered that it generates an opportunity for uncontrolled, out-of-hand entities to increase the level of fraud, the latter being in a much higher percentage (Haaland & Olden, 2022).

Is the financial and accounting security of entities increasingly threatened by these changes in the business environment, generated by the pandemic we have gone through and the necessity to integrate digital technology? In addition to the multiple benefits brought by the evolution of technology and the digitalization of professional activity, it is recognized that it has made companies' security vulnerable. Furthermore, despite the trend towards reducing financial fraud in the long term, the pandemic situation, resulting in a broad economic crisis, was a disruptive factor of the previously recorded trend in reported fraudulent phenomena (Karpoff, 2021).

Following surveys on companies affected by fraud between January 2020 and September 2021, it was found that more than half (52%) of the analysed topics confirmed that at least one of the factors determined by the COVID-19 pandemic was the cause of the destabilization of the entity's security, including: changes at organizational or operational level, reduction of internal controls, the transition to a work-from-home or hybrid system and, last but not least, the challenges brought by the boom in the use of digital technology, artificial intelligence (Association of Certified Fraud Examiners, 2022).

Given the above, it was necessary to use technology for our benefit, as we are in a position where we must learn to use intelligently the digital tools we have, in order to optimize the work process and remove the identified gaps, with reference to protecting the entity from a financial-accounting point of view, and not only, through artificial intelligence, combined with human intelligence.

It is worth mentioning that, by implementing anti-fraud software programs at the company/entity level, we will not reach a result of zero fraud, as it will subsist under any conditions, but for a reduced duration or in a much smaller number (ACFE, 2022).

The digitalization of the economy, the intensification of global conflicts, social distancing and remote work are just some of the factors that have led to the increase in cyber threats to private and public entities. Accounting is an essential department within each entity and thus requires constant improvement of the level of security, given that fraud often takes the form of theft of accounting information or distortion of its quality, the entity ending up taking decisions based on false accounting information or inaction where appropriate, thus incurring significant economic losses (Zadorozhnyi et al., 2021).

In order to mitigate the risk posed by the use of artificial intelligence to the security of entities, it is necessary for the EU to adopt specific legislation to support managers in maintaining control over the entity they manage (European Parliament, 2023).

Financial fraud is a real problem as people have come to use the opportunities and advantages of digitalisation for harmful purposes, such as money laundering and to multiply illicit financial transactions. The fight against financial crime is a difficult process precisely because it is unlimited, innovative and most often invisible (Sigetova et. al, 2022).

Social Economic Debates
Volume 14, Issue 1, 2025
ISSN 2360-1973; ISSN-L 2248-3837

Digital tools to detect and combat economic fraud

The fight against economic fraud never ceases to surprise us and stimulates us to always be ready for anything, as people's fantasy is endless and their ingenuity in doing harm, in order to increase their own income, is surprising, which is why new ways to combat this phenomenon must be constantly researched (Ghidotti et al., 2021).

Guaranteeing financial and accounting security through digital tools is a sine qua-non condition for public and private entities in today's unstable environment (Varnalii, 2022).

Currently, accounting and computer science are in a close relationship of dependence, looking from the perspective of the former. Accounting, considered an essential pillar within an entity, has constantly tried, during global changes, to keep pace with technological evolution and to be receptive to innovative solutions offered, or rather imposed, by it. Among the benefits of the positive approach to the technologization of the economic sphere are: accuracy and transparency of economic data, the ability to manage a large volume of data, removing errors, and also to process them in a timely and efficient manner, easy access to data and streamlining the information circuit, facilitating decision-making at management level (Bajan, 2018).

Poor cyber security of accounting data, especially managerial data, but also financial data, leads to the opening of the opportunity for unauthorized third parties to exploit them in order to obtain competitive advantages on the market, steal customers, contract with suppliers on more advantageous terms, predict future movements of the violated entity, charge more attractive prices, optimize their sales policy, strategy, etc. (Zadorozhnyi, 2021). Below are some examples of the consequences of the registration of economic fraud at entity level on stakeholders, who will inevitably lose confidence in it, for which collaborative relationships are most likely to suffer (see Figure no. 1).

Figure no. 1. The implications of economic fraud regarding the violated entity's relationship with interested parties

Source: created by authors

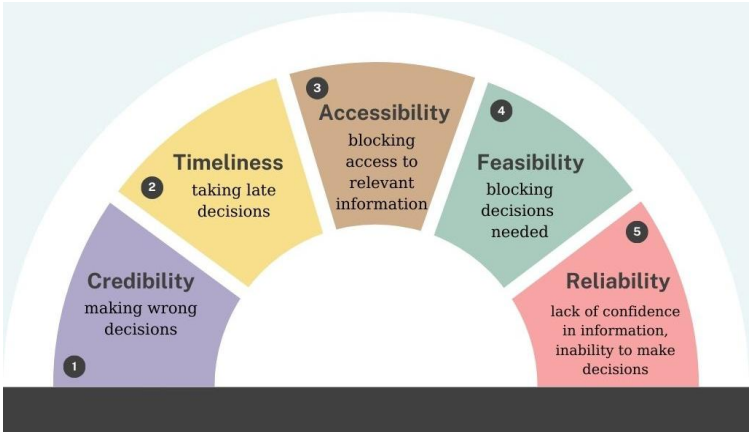
Social Economic Debates
Volume 14, Issue 1, 2025
ISSN 2360-1973; ISSN-L 2248-3837

The accountant of the future is considered the one who has the ability to understand technological changes, give them new valences thanks to his human contribution and be part of the new system (Yoon, 2020). Therefore, the accounting profession is and will be increasingly hybrid, as it combines, for maximum results with a minimum consumption of resources, specific human skills and functions offered by machines, robots (Gonçalves, Ferreira da Silva & Gonçalves Ferreira, 2022).

Although we would be tempted to say that the integration of information contributed by technology in the development of the accounting profession is something specific to the present, according to studies, this process of simplifying the professional life of the accountant and streamlining the quality of the work done by him began more than 140 years ago (Jasim & Raewf, 2020). However, it is true that, at present, the accounting profession has reached the highest level of technology so far, being easy to see the effects of the impact of the digital age.

We have briefly listed some of the countless advantages brought by digital technology, but we must not neglect the threats it entails. Thus, it is necessary to analyse the risks that implicitly come with the integration of digital technology, especially as regards fraudulent attacks directed against the financial and accounting security of the entity, distortion of the quality of accounting information, etc. (see Figure 2). Destabilizing the security of the entity through data breaching, loss, theft and multiple other fraudulent attitudes threatens its very survival (Gonçalves, Ferreira da Silva & Gonçalves Ferreira, 2022). New business conditions can lead to significant financial losses, assets or even loss of the ability to keep the business going, as well as lack of entrepreneurial potential, a situation in which the idea on which the business is based may become irrelevant for satisfying consumer needs, which are met by new technologies (Zachosova, 2022).

Figure no. 2. Cyber threats against the quality of accounting information



Source: created by authors

Artificial intelligence (AI) plays an important role in detecting and combating economic fraud, collecting information on identified financial fraud in a database is particularly important, as AI, based on machine learning algorithms, can identify certain prototypes and thus prevent them or predict how to combat fraudulent phenomena once installed (Yoon, 2020).

Social Economic Debates
Volume 14, Issue 1, 2025
ISSN 2360-1973; ISSN-L 2248-3837

Blockchain is one of the most widely used digital tools for detecting and combating economic fraud. This innovative technology uses encryption to eliminate the risk of falsification or manipulation of information and analyses the information recorded in the data base to outline and predict customer behaviour (Ren et. al., 2023).

In the field of accounting, Blockchain technology has had a considerable impact as it reduces costs, no longer having to use third parties to verify transactions, increases the quality of transparency information, and not only, the data distributed on the network is accessible to all users, but their modification can only be done following a protocol, and not unilaterally, which is visible to all those involved, and, above all, enhances transaction security (Lardo et al., 2022). By distributing the power of transaction verification among users and the high level of transparency, unauthorized data changes are prevented, fraudulent attempts are detected much easier and business performance is automatically measured (Alkafaji et. al, 2023).

The security of the entity is both threatened and protected by technology if used appropriately. Financial technology (called FinTech) has the ability to ease the control process and increase the efficiency of the entity's audit (Roszkowska, 2021). A great advantage of Blockchain technology is that it stores transaction history, which can be accessed quickly and easily whenever checks are needed. For example, in the great U.S. financial scandal concerning Enron, if Enron had recorded all transactions in the Blockchain database, the records would have been stored, unchanged, immutable, and associated with Enron, not SPEs (special purpose entities), which would have helped investors notice the entity's dangerous results in time and take appropriate action (Lardo et al., 2022).

But, inevitably, Blockchain technology also has minuses. For example, it was found that it is not created as an adaptive artificial intelligence system, because it is unable to detect asymmetric threats generated by banking phising, cloned technology, which can lead to the appearance of a user in a system as authentic.

Another digital tool for identifying and combating economic fraud is the Certified Threat Intelligence Analyst software package. With its help, fraudulent threats can be detected and analysed based on reports recorded in the database, as well as specific skills to identify and control them can be formed (Sigetova, 2022).

Also, to protect entities against fraudulent attacks, state-of-the-art cyber defence systems, developed on the basis of innovative and efficient algorithms, are needed. The network is protected thanks to firewalls, antivirus software, centralized markets are used at the level of smart devices such as App Store, Play Store, models are made to prevent and recognize illegal financial flows early, with the help of machine learning, which detects fraud through graphs, etc.

In Romania, in March 2023, the world's first "artificial" adviser was presented to help the Prime Minister, being called "ION" (viewed in the mirror, NOI) which was created by pro-bono Romanian specialists, with the purpose of supporting the Romanian Government in its connection with citizens and providing relevant information from them in order to make the most appropriate decisions (Ministry of Research, Innovation and Digitalization, 2023).

Among the most messages received from citizens through ION, an innovative digital tool on multiple levels, we find an increased interest in inflation (over 200,000 messages), as well as in aspects related to the economy (eg safety and food costs: 24% of interlocutors).

The project called ION, a worldwide pilot, created by Romanians for Romanians, is currently in the learning phase and can be (according to the authors) a ”public whistleblower” and a digital tool for detecting and, implicitly, combating economic fraud. All we have to do is tell him and teach him to have these concerns (given his function as a receiver to our problems and concerns).

Social Economic Debates
Volume 14, Issue 1, 2025
ISSN 2360-1973; ISSN-L 2248-3837

An innovative solution that can improve the financial-accounting field, proposed as an integral part of the FinTech concept, is that of Forensic Accounting/Forensic Accounting. For example, there are studies of how forensic accounting information is fraudulently disclosed through the social network Twitter, according to the world's four largest accounting firms, titled "The Big 4", namely: Deloitte, Ernst Young (EY), KPMG and PriceWaterhouseCooper (PwC) (Ultama et al., 2022).

Forensic accounting is a new way of combating economic fraud. Following a study on a relevant sample from South Africa, 3 aspects were identified on which banks should focus their attention in order to reduce financial and accounting fraud and prevent fraudulent attacks, namely: implementation of a code of conduct for both employees and customers of the entity, careful verification of hired personnel, with increased attention to newly employed personnel and adaptability to new technologies, implicitly befriending the entity's staff with what artificial intelligence involves (Akinbowale, 2023). These three aspects involve, in fact, the application of forensic accounting techniques, that is, similar to the forensic processes used in other fields (such as judicial or police), criminogenic patterns or profiles are sought to be taken into account by managers of financial and accounting entities when making decisions on liability in a financial-accounting partnership. These profiles can be the subject of a distinct scientific research, but here is emphasized the necessity for this concept to have legislative applicability, not only optional.

The more efficiently and thoroughly controlled the entity, the higher the security of the entity, thus protecting its primary interests, such as fighting unfair competition, reining in pressure exerted by authorities, eliminating or at least reducing erroneous and unfounded decisions, the entity being able to overcome the information threats with which it inevitably comes into contact (Horbachenko, 2020).

The European Union has noticed the risks that the use of artificial intelligence implies in terms of the financial and accounting security of the entity and not only, which is why, in April 2021, through the European Commission, it initiated the first regulatory framework regulating the risks generated by AI (European Parliament, 2023). By taking this measure, the EU aims to limit the possibilities of defrauding entities by exploiting technology in a negative way, ensuring the transparency of information systems, protecting the environment, etc., human capital playing a very important role in this regard.

Figure no. 3. Categories of risks involved in the use of AI identified by the EU

Source: created by authors

Social Economic Debates
Volume 14, Issue 1, 2025
ISSN 2360-1973; ISSN-L 2248-3837

The image above (see Figure 3) shows the four types of risks generated by the use of artificial intelligence, which the European Union regulated through the first draft law on this subject, which was proposed by the European Commission in April 2021, as I said, but on which Parliament expressed itself only in June 2023. The legislators are now in the negotiation stage to finalize the new legislation.

Regarding the unacceptable risk, which, indeed, holds the smallest weight, but which nevertheless must not be neglected, as it exists and is particularly dangerous, we list AI systems such as those that use subliminal manipulation techniques, those that aim to exploit vulnerable groups (people with disabilities, elderly people or children), those that identify biometric people in real time, but remotely, etc. High-risk AI systems are divided into two branches: those concerning the health or safety of the product (e.g. toys, medical devices), those concerning the 8 areas provided in the annex of the draft law; all of which require a preliminary EU assessment before being placed on the market, but also a systematic assessment if they have been accepted to be placed. Limited-risk AI systems are those that interact with humans, recognize emotions, manipulate images, audio or video content (e.g. chatbots, deepfakes).

Digitalization of the activity and control of public domain entities, in order to increase citizen's trust

Public institutions, unlike private entities, still have a fairly large volume of paper documents, which have not been entered into an IT system to be easily processed or shared, despite the fact that, at the moment, this progress is desired and considerable efforts are being made to achieve the objective.

Among the obstacles to the digitalization of the activity of public entities is the protection of citizens' personal data, which cannot be violated and must be managed with great care (Zhang et al., 2022).

Thus, many of the physical documents mentioned above, in order to be transmitted to other entities, require an anonymization procedure, which has often proved difficult, time-consuming and expensive. To this end, thanks to technology, we have identified a software called AGORA, which facilitates this task, but not only, as documents contain a wealth of untapped but important information that can reveal relevant data in the context of automated processing, which can create a valuable institutional database (Juez-Hernandez et al., 2023). The digital tool I just mentioned simplifies the work processes of other civil servants, who, even without having specific scientific knowledge, manage to analyse and extract important information from the documents assigned to them for resolution, AGORA being a great support for them especially in multidisciplinary projects, all the more so as it enjoys a very user-friendly interface. The AGORA program has been tested in the police and medical fields, resulting in only 1% of sensitive information being leaked (but which can be removed, and anonymization can be achieved perfectly through review by a human operator), but it can be applicable in any other field by developing new models in the database (Juez-Hernandez et al., 2023), all these efforts materializing in an increased degree of trust of citizens in the public system, as due to the careful anonymization of their personal data, the degree of fraud of public entities through unauthorized retrieval of sensitive data and their use for unauthorized purposes decreases.

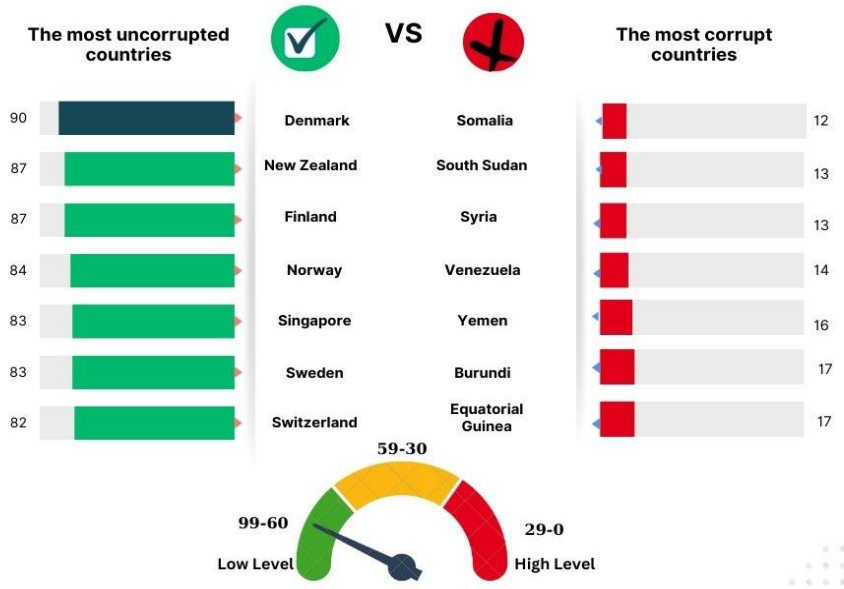
The nation undergoing a transformation process, such as the current situation, in which digitalization has taken over all professional fields and personal lives and imposed radical changes and rapid adaptation to new living conditions, is disturbed in a risky way if public administration and governance do not align with current needs, because citizens begin to fear the misappropriation of public funds, tax evasion, corruption at the level of public institutions (Dirir, 2023). A major impediment to the positive transformation of society is corruption, which

Social Economic Debates
Volume 14, Issue 1, 2025
ISSN 2360-1973; ISSN-L 2248-3837

is found at every step when we talk about public institutions and which, unfortunately, significantly impacts the financial sector.

According to statistics, among the most corrupt nations worldwide are Sub-Saharan Africa and Latin America (Dirir, 2023). Worldwide, countries are ranked according to the level of corruption identified by experts and reported by citizens on public sector institutions, from least corrupt to most corrupt, using a Corruption Perceptions Index, abbreviated as CPI (see Figure 4 for some examples), Romania is somewhere in the middle, with a CPI score of 46 in 2022, unlike 2021, when it had a score of 45, respectively in 2020 a score of 44, which signifies progress from this point of view.

Figure no. 4. Degree of corruption of the public sector in 2022, according to CPI



Source: created by authors

In order to combat economic fraud, corruption, the European Commission has proposed and offered free access to Member States managing EU funds a programme called Arachne. This program was developed using artificial intelligence and was created for the purpose of analysing the risks of possible fraudulent attacks, detecting conflicts of interest or any other disruptive elements, providing, at the beginning of each week, a risk index regarding the possibility of such irregularities regarding the management files of European funds (Villagrasa, 2022).

The digitalisation of the public sector can help anticipate citizens' needs and personalise the public services made available to them. Thus, high-performance and innovative information systems, artificial intelligence can lead to maximizing the applicability of citizens' right to good administration, transparency and promptness. But all these possible positive results are influenced and dependent on the good faith of public institutions, respectively of the people who make up the public sector of the country, because there is a risk of manipulating the decision-maker, citizens, when public administrations have imported databases and use artificial intelligence contrary to the purpose of ensuring and increasing the welfare of the population, but for personal interest.

Social Economic Debates
Volume 14, Issue 1, 2025
ISSN 2360-1973; ISSN-L 2248-3837

Following specialized studies, it was concluded that the ethical training of human staff has significant effects on the degree of compliance with values and principles, leading to the reduction of corruption of the public sector in the short term, but also in the long term if a training program in ethics and compliance of officials is periodically carried out at the level of the institution (Hauser, 2020). For example, one experiment, considered quite successful, was asking employees, before filling out a form, remembering the Ten Commandments and signing a truthfulness clause, as the results obtained revealed less dishonest behaviour on their part (Villagrasa, 2022). Thus, it was considered appropriate that when projects are underway, actions involving significant risks of fraud by staff to periodically communicate to them various messages of awareness of fraud risks, ethical and legal reminders, to awaken the conscience of officials and give rise to remorse, in order to repress illegal behavior.

Some authors argue that a good method of controlling the public sector would also be through whistleblowers, using a special helpline for this purpose, but officials are reluctant to report illegal behaviours they become aware of due to inadequate legal protection, risking losing their jobs (Alfordy, 2022).

Also, the transition to electronic platforms for declaring and paying taxes and fees was an important step in streamlining public sector control and increasing its financial-accounting security. These machine learning platforms offer the chance to use databases to prevent and combat economic fraud (Baghdasaryan, 2022).

The mission of the public sector, considering the need for digitization, is not only to support and implement the digital tools made available to it, but, above all, to ensure the transparency of public administration and a non-corrupt environment at the level of public institutions. Inadequate and inefficient control of public institutions leads to the development of the shadow economy, which is defined by all economic activities that are carried out in violation of the rules in force, in order to obtain unjustified material advantages and which cannot be controlled by the state (Němec et. al, 2022).

In addition to the aforementioned challenges, such as the high degree of corruption, fraudulent attacks, the pandemic situation, society is also facing numerous economic crises, environmental degradation, high-ranking challenges, which states are often not prepared to successfully overcome, their failure signifying nothing else than the decrease in the population's confidence in the public sector (Bodo, 2022).

Despite the fact that the public system constantly fights fraud, incurring impressive costs in order to prevent and combat it, we find at national level a huge fiscal gap, which affects not only the global economy, of the country, but also the well-being of citizens (Sigetova et al., 2022).

Conclusions

The COVID-19 pandemic was only an incentive to accelerate the digitization process, which the entire world would have gone through anyway, as it had already started and would have followed its natural course, but the pace would not have been as fast as the one imposed by the crisis situation we have just gone through.

The implementation of digital technology and the radical transformation of all previous activities of entities brought multiple benefits to employees, increasing labour productivity and saving the most limited human resource – time, however, also came with increased fraud threats and an increased vulnerability of the entity to these attacks that caused significant damage.

In any entity, decisions at management level are based on the information reported by the financial-accounting department, correlated with other information relevant to the given situation. Thus, the fraud of

Social Economic Debates
Volume 14, Issue 1, 2025
ISSN 2360-1973; ISSN-L 2248-3837

accounting data behind the information leads to inadequate, erroneous or late management decisions, thus recording not only considerable material losses, but even the possibility of ruining it.

The European Union has focused on the impact of digitalization on the security of entities, it is at an early stage of legislating, through the European Parliament, directives in the field, aiming to raise awareness and protect citizens and public and private entities against the risks generated by the use of AI, because capital markets are constantly fluctuating and adaptability through security is needed.

In this context, forensic profiles in the financial and accounting field should take into account the four types of risks legislatively identified by the European Parliament, namely unacceptable, high, limited and minimal.

We consider it to be impactful to develop a deontological code of employees at the level of each financial-accounting entity, aiming to create its own security structure that is able to engage in the fight against fraud from its onset, by knowing and identifying asymmetric risks deriving from economic fraud, generated by the online environment and to propose viable solutions to management staff adapted to the types of risks identified, in order to take appropriate decisions. In order to achieve such a code of ethics, inter-institutional discussions and consensus would be needed, and subsequently, based on the solutions found, legislative proposals would be advanced to engage the legislator in a public-private partnership and adopt measures valid for all those involved.

The health of an entity is strictly dependent on its degree of financial and accounting security, which is why tools should be developed, namely tools specifically designed to prevent and combat fraudulent attacks, financial crime. Digital technology offers multiple advantages and facilities that can be useful in the process of expanding the market of digital tools designed to ensure a high degree of control and security of the entity.

References

1. Akinbowale O.E., Klingelhöfer H.E. and Zerihun M.F. (2023), 'Application of forensic accounting techniques in the South African banking industry for the purpose of fraud risk mitigation', Cogent Economics &; Journal of Finance, 11(1), 2153412, https://doi.org/10.1080/23322039.2022.2153412
2. Alfordy F.D. (2022), "Effective fraud detection and prevention: perceptions among accountants and auditors in the public and private sectors in Saudi Arabia," Ekonomie a Management Journal, 25 (3), pp. 106-121, https://doi.org/10.15240/tul/001/2022-3-007
3. Alkafaji B.K.A., Dashtbayaz M.L. and Salehi M. (2023), 'The Impact of Blockchain on the Quality of Accounting Information: An Iraqi Case Study', Risks Journal, 11(58), https://doi.org/10.3390/risks11030058
4. Association of Certified Fraud Examiners. (2022), 'Occupational Fraud 2022: A report to the nations', Available at: https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf, accessed December 2023
5. Baghdasaryan V., Davtyan H., Sarikyan A., and Navasardyan Z. (2022), 'Improving Tax Audit Efficiency Using Machine Learning: The Role of Taxpayer's Network Data in Fraud Detection', Applied Artificial Intelligence Journal, 36(1), 2012002, https://doi.org/10.1080/08839514.2021.2012002
6. Bajan M. (2018), "The impact of information technologies on accounting", Accounting and auditing in globalized conditions: realities and development perspectives Journal, 7, pp. 242-249

Social Economic Debates
Volume 14, Issue 1, 2025
ISSN 2360-1973; ISSN-L 2248-3837

7. Bodo B. and Janssen H. (2022), "Maintaining Trust in a Technological Public Sector," Policy and Society Journal, 41 (3), pp. 414-429, https://doi.org/10.1093/polsoc/puac019
8. Corruption Perceptions Index (2022), https://www.transparency.org/en/cpi/2022, accessed January 2024
9. Dirir S. A. (2023), 'The role of impartial administration in financial sector performance: a comparative study of Latin America and Sub-Saharan African countries', Financial Internet Quarterly, 19(3), pp. 16-30, https://doi.org/10.2478/fiqf-2023-0016
10. European Parliament (2023), https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf, accessed January 2024
11. Ghidotti M., Papoci S., Dumitraşcu C., Zdiniakova T., Fiamegos Y., and Beatriz de la Calle Gutiñas M. (2021), "ED-XRF as a screening tool to assist customs laboratories in their fight against fraud. Stat-of-the-art", Talanta Open Journal, 3, 100040, https://doi.org/10.1016/j.talo.2021.100040
12. Gonçalves M. J. A., Ferreira da Silva A. C. &; Gonçalves Ferreira C. (2022), "The future of accounting: how will digital transformation affect the sector?", Informatics Journal, 9, 19, https://doi.org/10.3390/informatics9010019
13. Haaland I. and Olden A. (2022), "Fraud Concerns and Support for Economic Aid Programs," Journal of Economic Behavior and Organization, 203, pp. 59-66
14. Hauser C. (2020), "From Preaching to Behavior Change: Promoting Ethics and Conformity Learning in the Workplace," Journal of Business Ethics, Springer, 162 (4), pp. 835-855, https://doi.org/10.1007/s10551-019-04364-9
15. Horbachenko S. (2020), "Cybersecurity as a component of Ukraine's economic security", Galician Economic Journal, 66 (5), pp. 180-186, https://doi.org/10.33108/galicianvisnyk_tntu2020.05.180
16. Jasim Y. and Raewf M. (2020), "The Impact of Information Technology on the Accounting System," Journal of Humanities and Social Sciences, 4 (1), pp. 50-57, https://doi.org/10.24086/cuejhss.v4n1y2020.pp50-57
17. Juez-Hernandez R., Quijano- Sánchez L., Liberatore F. and Gómez J. (2023), "AGORA: An intelligent system for anonymization, information extraction, and automatic mapping of sensitive documents," Applied Soft Computering Journal, 145, 110540, https://doi.org/10.1016/j.asoc.2023.110540
18. Karpoff M. J. (2021), "The Future of Financial Fraud," Journal of Corporate Fiance, 66, 101694, https://doi.org/10.1016/j.jcorpfin.2020.101694
19. Lardo A., Corsi K., Varma A., & Mancini D. (2022), "Exploring blockchain in the accounting domain: a bibliometric analysis", Accounting, Auditing &; Accountability Diary, 35 (9), pp. 204-233, https://doi.org/10.1108/AAAJ-10-2020-4995
20. Ministry of Research, Innovation and Digitalization (2023), https://www.mcid.gov.ro/premiera-romaneasca-ion-primul-consilier-guvernamental-din-lume-ce-va-folosi-inteligenta-artificiala-9546/, accessed January 2024
21. Němec D., Machová Z., Kotlán I., Kotlánová E. and Kliková C. (2022), 'Corruption in public administration as a brake on the transition to Industry 4.0', Sage Open Journal, 12(1), https://doi.org/10.1177/21582440221085009

22. Ren Y., Ren Y., Tian H., Song W. & Yang Y. (2023), "Improving transaction security through blockchain-based fraud protection", Connection Science Journal, 35 (1), 2163983, https://doi.org/10.1080/09540091.2022.2163983
23. Roszkowska P. (2021), "Fintech in Financial Reporting and Auditing to Prevent Fraud and Protect Capital Investments," Journal of Accounting and Organizational Change, 17 (2), pp. 164-196, https://doi.org/10.1108/JAOC-09-2019-0098
24. Sigetova K., Uzikova L., Dotsenko T., and Boyko A. (2022), "Recent Trends in World Financial Crime," Financial and Credit Activity: Problems of Theory and Practice Journal, 5 (46), pp. 258-270, https://doi.org/10.55643/fcaptp.5.46.2022.3897
25. Tilea D.M., Nicolau I., Dinu A.M. (2023), "Managing Uncertainty: Using AI to Effectively Reduce Risk", Social Economic Debates, Volume 12, Issue 1, https://www.economic-debates.ro/Art.%205%20Tilea%201%202023.pdf
26. Utama A.A.G.S. and Basuki B. (2022), "Exploring Theme-Based Twitter Data in Forensic Fraud Accounting Studies," Cogent Business &; Management Journal, 9 (1), 2135207, https://doi.org/10.1080/23311975.2022.2135207
27. Varnalii Z. and Mekhed A. (2022), 'Business entities' financial security under digital economy', Financial and credit activity: problems of theory and practice Journal, 4(45), pp. 267-275, https://doi.org/10.55643/fcaptp.4.45.2022.3813
28. Villagrasa O.C. and Solé J.P. (2022), "Nudging e inteligencia artificial contra la corrupción en el sector público: posibilidades y riesgos", Revista Digital de Derecho Administrativo, 28, pp. 225-258, https://doi.org/10.18601/21452946.n28.08
29. Yoon S. (2020), "A Study on the Transformation of New Technology-Based Accounting: Evidence from Korea," Sustainability Journal, 12 (20), 8669, https://doi.org/10.3390/su12208669
30. Zachosova N., Kutsenko D. and Koval O. (2022), "Strategy and mechanism of financial and economic security management of enterprises in conditions of war, Industry 4.0 and the Money World", Financial and Credit Activity: Problems of Theory and Practice Journal, 4 (45), pp. 223-233, https://doi.org/10.55643/fcaptp.4.45.2022.3819
31. Zadorozhnyi Z.M., Muravskyi V., Shevchuk O., & Bryk M. (2021), "Innovative accounting methodology ensuring economic interaction and cybersecurity of enterprises," Marketing and Management of Innovations Journal, 4, pp. 36-46, https://doi.org/10.21272/mmi.2021.4-03
32. Zhang G., Zhu X., Li Y., Pedrycz W., and Li Z. (2022), "Granular data representation under privacy protection: Tradeoff between data utility and privacy via information granularity," Applied Soft Computering Journal, 131, 109808, https://doi.org/10.1016/j.asoc.2022.109808