Regulatory Cybersecurity in the European Union and the Republic of Moldova

Liudmila LAPIȚKAIA[*], Alexandru LEAHOVCENCO[**]

Abstract

The rapid development of information technology leads to various opportunities for both individuals and businesses to conduct including financial transactions through the Internet. In such circumstances, cyber security issues become very relevant. In this regard, the European Parliament regularly reviews and updates the cybersecurity regulatory framework. In turn, the Republic of Moldova should also update its legislative framework in the field of cyber security in order to bring it in line with European standards. On the basis of this analysis, the normative documents on cyber security of the Republic of Moldova are considered and the directorates for further development of cyber security in Moldova are established.

Key words: cyber security, Cybersecurity act, the NIS Directive, the National Cyber Security Program of the Republic of Moldova.

JEL Code: Y80

1. Introduction

The dynamic formation of a global information space is connected, on the one hand, with the provision of unprecedented information capabilities to humanity, as well as with the emergence of new threats. A new cybersecurity phenomenon has emerged. Various cybersecurity definitions can be found in the specialized literature. For example: in accordance with the provisions of the Cybersecurity act adopted by the European Parliament on 12 March 2019 *«cybersecurity means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats»*. In according to the definition given by The Economic Times: «Cybersecurity or information technology security are the techniques of protecting computers,

[*] Liudmila LAPIȚKAIA is associate professor at Academy of Economic Studies of Moldova, Chisinau, E-mail: liudmila@ase.md

[**] Alexandru LEAHOVCENCO is PHd student at Academy of Economic Studies of Moldova, Chisinau, E-mail: alexandru.leahovcenco@yandex.com

networks, programs and data from unauthorized access or attacks that are aimed for exploitation. (Economic Times)

Description: Major areas covered in cybersecurity are:

1) Application Security,
2) Information Security,
3) Disaster recovery,
4) Network Security».

One of the best-known cyber security firms in Russia, Kaspersky, gives the following definition: «*cyber-security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories*.

- *Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.*
- *Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.*
- *Information security protects the integrity and privacy of data, both in storage and in transit.*
- *Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.*
- *Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.*
- *End-user education addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization». (Kaspersky)*

American company Cisco on it's web page published the following definition: «cybersecurity is the practice of protecting systems, networks, and programs from digital attacks».(Cisco)

Also, ENISA differentiates the following areas of cybersecurity (ENISA,2015,p.11):

Analysing all this information, the authors synthesized the following definition of cyber-security: cyber security is the organization of protection of various information systems and their carriers from cyber-attacks.

Table 1. Different domains of Cybersecurity

Communications Security	Protection against a threat to the technical infrastructure of a cyber system which may lead to an alteration of its characteristics in order to carry out activities which were not intended by its owners, designers or users.
Operations Security	Protection against the intended corruption of procedures or workflows which will have results that were unintended by its owners, designers or users.
Information Security	Protection against the threat of theft, deletion or alteration of stored or transmitted data within a cyber system.
Physical Security	Protection against physical threats that can influence or affect the well-being of a cyber system. Examples could be physical access to servers, insertion of malicious hardware into a network, or coercion of users or their families.
Public/National Security	Protection against a threat whose origin is from within cyberspace but may threaten either physical or cyber assets in a way which will have a political, military or strategic gain for the attacker. Examples could be 'Stuxnet' or wide-scale DOS attacks on utilities, communications financial system or other critical public or industrial infrastructures.

Source: The European Union Agency for Network and Information Security

2. Literature review

The presence of the Internet and the development of digital technologies are dynamically changing the usual spheres of human life, transforming the economy, making it digital. The scale of changes and its innovative significance are so significant that in the European Union they believe that nation states cannot cope with the problems of ongoing transformations due to their limited capabilities. Coordinated policies and general legal frameworks are needed. These arguments formed the basis for the creation of the European Union Single Digital Market Strategy (Digital Single Market), which was presented in the Communication by the European Commission in 2015.

The main documents in the field of cybersecurity in Europe are:

1) The Directive on security of network and information systems (the NIS Directive) was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016.
2) Regulation of the European parliament and of the council on ENISA, the "EU cybersecurity agency", and repealing regulation (EU) 526/2013, and on information and communication technology cybersecurity certification ("Cybersecurity act") adopted at 12 march 2019, during the European Parliament plenary , entering into force 20 days after its publication in the Official Journal of the European Union.

After analysing cyber threats, Europol in its report "Assessment of threats from organized crime on the Internet" (The 2017 Internet Organized Crime threat Assessment (IOCTA)) noted that there is a noticeable convergence of interests of cybercrime and organized crime, using the opportunities of the shadow digital economy, which leads to the conclusion that attacks on various databases, both personal and corporate will become more sophisticated.

The Directive on network and information security (the Directive on security of network and information systems (NIS Directive)) was adopted in 2016 to improve supranational regulation of countering cyber-attacks on critical infrastructure. Until May 2018, EU member States had to incorporate its provisions into their national legislation. EU member States should adopt national cybersecurity strategies that define strategic objectives, appropriate policies and regulatory measures in this area. The Directive also provides for the establishment of a "cooperation Group" to facilitate cooperation and exchange of information among member States, including through the preparation of guidance documents to facilitate the implementation of the provisions of the Directive relating to life support services operators (operators of essential services).

An important provision of the Directive is the establishment of a Network of computer security incident response teams (CSIRTs). The network should include relevant units in each of the EU member States. The European Agency for network and information security (ENISA) will actively support cooperation between these groups.

The Directive also establishes certain obligations towards non-state actors. Enterprises have an important role in society and the economy, is designated in the Directive as "operators of services of critical infrastructure" (these include, in particular, digital infrastructure) should ensure adequate levels of digital security of their services and to notify serious incidents to the appropriate national authority. These obligations are imposed on providers of digital services.

The Directive on network and information security (the Directive on security of network and information systems (NIS Directive)) was adopted in 2016 to address gaps in European regulation of countering attacks on critical infrastructure. Until May 2018, member States should implement its provisions in their national legislation. In particular, they will need to adopt national cybersecurity strategies that define strategic objectives, relevant policies and regulatory measures. The Directive also provides for the establishment of a "cooperation Group" to facilitate strategic cooperation and exchange of information among member States, including through the preparation of guidance documents to facilitate the implementation of the provisions of the Directive relating to life support services operators (operators of essential services)

The Directive establishes the establishment of a Network of computer security incident response teams (CSIRT). The network should include relevant units in each of the EU member States. The European Agency for network and information security (ENISA) actively supports cooperation between these groups.

In addition to obligations for EU member States, the Directive also establishes certain obligations towards non-state actors. Enterprises have an important role in society and the economy, is designated in the Directive as "operators of services of critical infrastructure" (these include, in particular, digital infrastructure) needs to provide the appropriate level of cyber security of their services and to notify serious incidents to the appropriate national authority. These obligations are imposed on providers of digital services.

Thus, the NIS Directive has become the basis of European cooperation to combat serious incidents in the digital space and contribute to improving the conditions for the development of interactions.

3. Analysis of regulations in the field of cyber security of the European Union and the Republic of Moldova

The main task in the field of cyber security is the protection of personal data. In 2016, in the framework of the changing legal regulation of this sphere was adopted by the General regulation on data protection (General Data Protection Regulation (GDPR)), which replaces EU Directive on data protection 95/46/EC, which entered into force on 25 may 2018. This Regulation is intended to protect the rights of individuals with respect to the processing of personal data by all companies offering their services on the European market. Thus, the GDPR applies, among other things, to companies located outside the EU, whose personal data processing activities are related to the supply of goods and services to data subjects in the EU. The regulation establishes multi-level sanctions for violations of data protection legislation.

In 2016, the European Commission and the European cybersecurity organization (ECSO) signed a partnership agreement on cybersecurity in order to implement the tasks related to cybersecurity outlined in the Strategy of building a Single digital market. The Treaty aims to promote competitiveness and innovation in digital security in the private sector. ECSO includes more than 200 members, including large companies in the field of cybersecurity, small and medium enterprises, and start-ups, research centers, universities, clusters and associations.

In 2017, the European Commission also proposed the establishment of a new body, the EU cybersecurity Agency, on the basis of ENISA, with the simultaneous establishment of a pan-European network for certification of information and communication technology products and services.

One of the key conditions for creating a stable functioning Single digital market is to ensure cybersecurity. The most important area of regulation, to which the EU pays special attention, is to ensure the safety of critical infrastructure.

The Cybersecurity Act:

- Strengthens the ENISA by granting to the agency a permanent mandate, reinforcing its financial and human resources and overall enhancing its role in supporting EU to achieve a common and high level cybersecurity.
- Establishes the first EU-wide cybersecurity certification framework to ensure a common cybersecurity certification approach in the European internal market and ultimately improve cybersecurity in a broad range of digital products (e.g. Internet of Things) and services.

The Ministry of Information Technology and Communications of the RM, jointly with the relevant authorities, developed the National Cyber Security Program of the Republic of Moldova. The document was adopted by Government Decision No. 811 of 29 October 2015.

This document is based on the provisions of the National Strategy for information society development "Digital Moldova 2020" strategy and the national security Strategy of the Republic of Moldova. The National Cyber Security Programme includes 7 areas of intervention:

- secure processing, storage and data access;
- security and integrity of electronic communications networks and services;
- emergency prevention and response capabilities (CERT);
- preventing and combating cybercrime;
- strengthening cyber defence capabilities;
- education and information;
- international cooperation and interaction.

This document has been prepared in accordance with the provisions of the Association Agreement, the Republic of Moldova and the European Union, the Council of Europe's Convention on cyber-crime Strategy, the cyber security of the European Union and the Recommendations of the International Telecommunication Union relating to the cyber security of the electronic communication networks.

Secure processing, storage and data access envisage:

1) the ensuring compliance with the legal and regulatory framework on cybersecurity of the Republic of Moldova, which will include:

- definition of cybersecurity terms (concepts) ;
- delineation of competencies by area;
- the establishment of the authority with functions to monitor the compliance of cybersecurity;
- appointment of authority to scrutinize the implementation of audit results in the field of cybersecurity;
- obligations of holders of public information systems to periodically audit these systems, establishing the frequency, levels and reporting to the competent authority;
- establishment of an inter-sectoral Council on cybersecurity (with the function of coordinating cybersecurity activities)

2) Classification of types of information, except for state secrets,

3) Analysis and development of proposals for the application at the national level of standards related to the processing, storage and safe access to data in accordance with the classification of types of information considered in the technical committees on standardization TC 28 "Information technology" and TC 29 «Electronic communications»,

4) Development of a methodology for assessing the vulnerability of public information systems based on defined, adopted and approved standards,

5) Development of mandatory minimum cybersecurity requirements,

6) Certification of specialists of standards and methodologies, and approved mandatory minimum requirements of cybersecurity,

7) Definition and planning in budgets of institutions of the financial means necessary for carrying out audit of cybersecurity on the basis of the approved methodology.

Security and integrity of electronic communications networks and services establishes the need to:

- bring electronic communications legislation into line with the EU framework directives in this area,
- establish minimum security measures to be taken by suppliers to ensure the security, reliability and integrity of electronic communications networks and/or services and reporting incidents with significant impact on them,
- analysis and implementation at the national level of European and international standards relating to the protection and security of electronic communication networks and their transfer to the National Institute for standardization,
- conduct research on amendments to the legislation on electronic communications in order to eliminate or reduce the number of impersonal subscribers of electronic communications services,
- develop of a special communication network of public administration bodies on the whole territory of the Republic of Moldova.

Emergency prevention and response capabilities (CERT) provides for the following actions:

- creation of a National Cyber Incident Response Center (CERT),
- creating a national cyber incident alert and information system in real time,
- creation of departmental response centres for cyber incidents in the central and local public administration authorities, other institutions that are holders of state information systems,
- establishment for central and local public administration authorities and the business environment in the field of information and communication technologies for mandatory operational reporting on cyber incidents based on a data exchange mechanism and clearly defined roles,
- database organization, with access by responsible authorities, identified or registered cybernetic threats, vulnerabilities and incidents, technologies and methods used for attacks, best practices for protecting the information and communications technology industry,
- Conduct joint exercises and training sessions to strengthen the response capacity to cyber-attacks, including blocking simulated cyber-attacks.

Such a position as Preventing and combating cybercrime sets the following:

- development of a draft law on introducing amendments and additions to criminal legislation and legislation on offenses to prevent and combat cybersecurity information in order to continuously harmonize it with the provisions of the European Convention on Information Crime and the decisions of the Committee of this Convention,
- training of law enforcement officers, specialists certified in the field of cybersecurity,

- implementing the recommendations of the Council of Europe, in particular, the EAP project on training law enforcement personnel,
- development and approval of the draft law on ratification of the Additional Protocol to Council of Europe's Information Crime Convention.

Strengthening cyber defence capabilities directed to:

- develop a section on cyber defence of the Republic of Moldova, as part of the Information Security Strategy of the Republic of Moldova,
- establish of responsible bodies and mutual cooperation in peacetime, in situations of crisis, siege and war in cyberspace,
- use the power of cyberspace to advance national interests, values and goals in cyberspace,
- develop of military capabilities to protect critical infrastructure and services for national defence.

Such a direction as *Education and information* provides development of the concept of information and risk awareness campaigns in cyberspace and supplement of the curriculum in the field of cybersecurity.

International cooperation and interaction aimed at conclusion of cooperation agreements with other national cyber security incident response teams (CERT), as well as US–CERT, European and North Atlantic (NATO NCERT) and creation of a platform for coordination and consulting in the field of cyber threat assessment and search for solutions.

4. Conclusions

In conclusion, it should be noted that the authors analysed the literature on the specialty in terms of the definition of cybersecurity offered their definition, namely: cyber security is the organization of protection of various information systems and their carriers from cyber-attacks.

Having analysed the regulatory framework in the field of cybersecurity of the European Union and the Republic of Moldova, we can state the following:

1) In the light of the changes in the European legislation in the field of cybersecurity, the Republic of Moldova should also update its normative and legislative acts in this field,
2) Moldova should update its critical infrastructure to maintain high level of cyber security against the threats of modern cyberattacks,
3) It is necessary to create a state body for cybersecurity such as the Moldovan cybersecurity Agency that would accumulate a database of cyber threats and take appropriate emergency measures to localize them.

References:

Cisco https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

ENISA Definition of Cybersecurity Gaps and overlaps in standardization, December 2015

European Parliament legislative resolution of 12 March 2019 on the proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") - http://www.europarl.europa.eu/doceo/document/TA-8-2019-0151_EN.html?redirect#BKMD-20,

Hotărîre Guvernului al RM Nr. 811 din 29.10.2015 cu privire la Programul național de Securitate cibernetică a Republicii Moldova pentru anii 2016-2020 http://lex.justice.md/viewdoc.php?action=view&view=doc&id=361818&lang=2

The Economic Times https://economictimes.indiatimes.com/definition/cyber-security

Kaspersky https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

The effects of cloud technology on management accounting and decision making, Volume 10 – Issue 6, https://www.cimaglobal.com/Research--Insight/The-effects-of-cloud-technology-on-management-accounting/.

Decentralized Applications - Harnessing Bitcoin's Blockchain Technology, by Siraj Raval : O'Reilly Media Release, July 2016 p 118,

“Big data: science in the petabyte era” Nature 455 (7209): 1, 2008.

Douglas and Laney, “The importance of ‘big data’: A definition,” 2008.

Barlow J. P. Selling Wine Without Bottles: The Economy of Mind on the Global Net: http://lib.ru/COPYRIGHT/barlou.txt.

Parinov S.I, Yakovleva T.I, Economy of the 21st century based on Internet technologies.

Big Data: Principles and Best Practices of Scalable Realtime Data Systems, by Nathan Marz, James Warren, p 328, 2015.

Computer Networking: A Top-Down Approach (6th Edition), by James F. Kurose, Keith W. Ross, p 880, 2012

Assessment of the Internal Governance as an Element of the Supervisory Review and Evaluation Process (SREP)

Anastasia BEJAN*

Abstract

In recent years, the internal governance issues in the banking sector have received increased attention on the international level. One of the global financial crisis causes was banks' weak and superficial internal governance practices. Before the financial crisis, banks have not effectively implemented the internal control mechanisms and risk management, because the goal of profit maximization prevailed and conditioned the banks managers to take the decisions with a high degree of risk. The European Banking Authority (EBA) is constantly concerned with issuing the best policies for an efficient banking supervision in the European countries. In this context, EBA included the internal governance assessment as a component of the Supervisory Review and Evaluation Process (SREP). The difference between the previous researches on the internal governance topic and the present article is the fact that it analyzes the peculiarities of the internal governance assessment during the SREP process, performed by the supervisory authority. The supervisory authority task is to assess whether or not a bank's internal governance arrangements are adequate for and correspond to the institution's risk profile, business model, size and complexity. The score assigned following the internal governance assessment expresses the supervisory authority view on the adequacy of the institution's internal governance arrangements and institution wide controls.

Keywords: banks, banking supervision, internal governance, internal control, risk management

JEL Code: G21; G34

1. Introduction

Getting profit is the main objective of the management of a bank. The tendency of profit maximization can often make the banks to ignore the risk level in order to achieve a bigger profit. If a bank's management is a qualified one, it will be aware that the registration of high performance does not mean stability of the bank and the safety of the decisions taken.

One of the main tasks of banking supervision is to ensure the sustainability and viability of credit institutions. In the framework of the SREP evaluation, the supervisory determines the quality

* Anastasia BEJAN, National Bank of Moldova, E-mail: anastasia.bejan@yahoo.com

of the strategies, processes and mechanisms implemented by banks and the sufficiency of their own funds and liquidity to ensure the coverage of all risks.

The Guidelines on common procedures and methodologies for the supervisory review and evaluation process, published by the European Banking Authority in December 2014, cover in details all aspects of the SREP process. The overall result of SREP gives to the bank an evaluation score, which represents the supervisory assessment of the institution's risk profile and viability.

The term internal governance refers to the internal organization of a bank's activity and the way it develops and manages its business and risks.

In the context of the SREP Guidelines, the internal governance includes the general framework of the administration of a bank's activity, organization and functioning of the management body, organization of the internal control functions of the bank, organization of the risk management framework, etc.

Although different researchers assessed the internal governance topic, the present article addresses a different approach of this term, by its analysis within the SREP framework. The internal governance analysis within the SREP framework differs from the traditional analysis of the internal governance, as the supervisory review and evaluation process requires a very deep assessment of this element, as all the findings should be relevant in order to justify the score given to the institution.

The article is organized in four main parts that focus on the internal governance assessment during the SREP process:

- The first part is dedicated to a succinct literature review of internal/corporate governance, identifying, among numerous definitions, the key-features of this term.

- The second part focuses on the assessment of the banking management framework as a part of the internal governance, including aspects concerned with organizational structure and organization and responsibilities of the management body.

- The third part reveals the assessment of the internal control functions, such as internal audit, risk management and compliance.

- The fourth part emphasizes the assessment of the quantitative aspects of the internal governance, including the risk management framework, risk appetite and the Internal Capital Adequacy Assessment Process (ICAAP).

2. Literature review

In the extremely vast economic literature devoted to this topic, analysis of various aspects of internal/corporate governance can be encountered, thus showing the complexity of this term.

Concerning the definitions of the internal/corporate governance, there is not a single definition of this term rather it might be viewed from different angles. Among the first definitions, the corporate governance was defined as ,,the ways in which suppliers of finance to corporations assure themselves of getting a return on their investment" (Shleifer and Vishny, 1997).

Organization for Economic Co-operation and Development (OECD) in 1999 defined corporate governance as ,,the system by which business corporations are directed and controlled. The corporate governance structure specifies the distribution of rights and responsibilities among different participants in the corporation, such as, the board, managers, shareholders and other stakeholders, and spells out the rules and procedures for making decisions on corporate affairs".

Another researcher defined the internal governance as ,,the processes, customs, policies, laws and institutions that direct the organizations and corporations in the way they act, administer and control their operations" (Khan, 2011).

According to the EBA Final Report on Guidelines on internal governance (EBA/GL/2017/11), internal governance includes all standards and principles concerned with setting an institution's objectives, strategies and risk management framework. It also focuses on how the business is organized; how responsibilities and authority are defined and clearly allocated; how reporting lines are set up and what information they convey; and how the internal control framework is organized and implemented, including accounting procedures and remuneration policies.

The corporate governance was also examined from the point of view of 2 core aspects: internal and external. Internal aspects include ownership structure, the board of directors and committees, internal control, risk management, transparency and financial reporting. External aspects can either be market-oriented, or can take the form of credit ranking, and/or social requirements (Naciri, 2009).

There can be emphasized 3 pillars of corporate governance: transparency (allowing to be observable to outsiders the processes and transactions of a company), accountability (building integrity in a company), and security (a company is expected to make their processes transparent and their people accountable while keeping their enterprise data secure from unauthorized access) (Roman, 2019).

Regarding the internal governance in the banking sector, the KPMG audit company (2018) in the article ,,Internal governance: Addressing weaknesses" mentioned that the internal governance remains a key area of focus for European banking supervisors, playing a fundamental role in maintaining the stability and reliability of individual institutions and the entire banking system.

Supervisory authorities must require institutions to have an adequate risk management processes and internal control mechanisms, including sound reporting and accounting procedures in order to identify, measure, monitor and control all the transactions.

3. Banking management framework

The assessment of the inherent risks of the banking management framework has more a qualitative nature than quantitative nature. When assessing this type of risk will be initially collected information and documents about the management body of the bank (executive body, council and its specialized committees), paying closer attention on the bank's organizational structure, the powers, responsibilities, composition and functioning of the management body, the degree of adequacy of the

bank's administrators (composition, qualification, experience). As well, will be assessed if the bank has a clear organizational structure, with well-defined, transparent and correct lines of responsibility and if the persons that hold key functions in the bank are properly identified and evaluated.

In order to establish properly the score for the internal governance and institution-wide control arrangements, the supervisor should answer the following key-question: Are the internal governance and institution-wide control arrangements adequate for the identification, management, monitoring, reporting and reducing the risks, given the nature, the magnitude and the complexity of the bank?

3.1. The organizational structure

It is important to have a general understanding of the way is organized the bank's activity. In this regard, will be analyzed the organizational structure of the bank, including if there is a clear delimitation between the business lines, business units, staff with key-functions and the structure of the reporting units. The supervisor will assess if the organizational structure is clear, with well-defined, transparent and correct lines of responsibility. A comprehensive understanding of the way is organized and function the bank's activities is essential for the assessment of the adequacy of the internal governance processes and the internal control mechanisms, as well as their adequacy depending on the structure, business and risks assumed by the bank.

In order to analyze the organizational structure of the bank, will be assessed if the bank has a well-defined organizational structure and if at the establishment of the banking activity management framework is taken into account the nature, the magnitude and the complexity of the inherent business model risks. For the same purpose, will be evaluated if the bank's staff is properly selected and is performing its activities according to its duties. Also, will be analyzed the ownership structure of the bank, its structural changes, the identity of the direct and indirect shareholders', including the beneficiary owners.

3.2. Organization and responsibilities of the management body

The council is the management body of the bank, which has supervisory duties of bank performance, approval and monitoring of implementation of strategic objectives, governance framework and corporate culture by the executive body, and is responsible for overall bank activity.

When assessing the adequacy of the council members will be assessed if the members:

1) are aware of the structure of the management body and distribution of the duties and responsibilities between the executive body, the council and its specialized committees

2) ensure the compliance with the experience and knowledge on individual and collective level

3) perform their tasks with honesty, objectivity and loyalty, dedicate enough time and caution in their performance and in strict compliance with the legal framework

4) actively participate in the activity of the bank and are able to take decisions and make their own sound, objective and independent judgments

5) define and understand the organizational structure of the bank, the ICAAP and the general framework for crisis simulations.

The bank should have 4 specialized council committees: Audit Committee, Risk Management Committee, Appointment Committee and Remuneration Committee.

When assessing the adequacy of the specialized committees' members, will be analyzed the following aspects:

1) In case of assessing the Audit Committee: the independency of the head of Audit Committee and the performance of the Committee duties according to the provisions of the Regulation on banking activity management framework.

2) In case of assessing the Risk Management Committee: the given support to the council regarding the current and future risk appetite and risk strategy of the bank, regarding the establishment of the nature, volume, format and frequency of the information concerning the risks and monitoring the appliance of this strategy by the executive body.

3) In case of assessing the Appointment Committee: the relevant experience concerning the process of selection and evaluation of the adequacy of the candidates for the positions in the management body of the bank and key-functions.

4) In case of assessing the Remuneration Committee: the realization of duties with competence and independence, the relevant experience regarding the remuneration policies and practices, risk management and/or audit/controlling activities, especially concerning the mechanism for alignment the remuneration structure at the bank's risk and capital profile.

The executive body is in charge of managing the current business of the bank, reports to the council and shall ensure proper implementation of the bank's management framework, develop and approve secondary bylaws, where appropriate.

When analyzing the efficiency of the management of the current banking activity, will be assessed the professional standards, the quality of the collective decision making process and the uniform distribution of the duties, as well as the extent to which the members of the executive body are aware of the newest activities of the bank. These aspects will be assessed by the analysis of the quality of the executive body reports and minutes of the meetings, including the examination of their decisions.

At this stage will be assessed if the executive body of the bank maintains efficient policies for the identification, evaluation, management and mitigation or prevention the current and potential conflicts between the bank's interests and the private interests of the staff and management body.

Also, will be assessed if the members of the executive body have the professional reputation and necessary knowledge and experience in the field of activities allowed to the banks, as well as sufficient skills for performing the duties in the bank.

The supervisor will assess if the executive body takes decisions based on sound information, which does not contradict the bank's strategies, encourages sound and prudent management and does not threaten the bank's financial soundness and the legal interests of the interested parts. As well, will be verified if the decision-making process of the executive body cannot be dominated by one person or a group of persons, and the decisions are taken in an objective and impartial way and follow the bank's interests and not the personal one.

4. Internal control mechanisms

Internal control functions shall include a risk management function, a compliance function and an internal audit function. The risk management and compliance function shall be verified by the internal audit function.

4.1. Internal audit function

The organizational structure of the bank should be organized so as to make sure that the internal audit function is not directly involved in the operational organization of the bank and that the auditors are independent and do not perform operational tasks that enter in the sphere of activities that are under their control and/or monitoring. However, the audit function should actively cooperate with other functions, relevant committees and bank's subdivisions, in the extent to which this activity is according to its tasks and level of independency.

The supervisor will assess if the audit function performs its activity in accordance with the internal regulation on the internal audit, approved by the bank's council that includes information about the way of organization, rights and responsibilities, cooperation with other bank's subdivisions.

As well, will be assess the nature and the scope of the audit, in order to ensure that it covers efficiently and extensively the bank's activities and risks, including the outsourced activities.

The supervisor will assess if the audit function has sufficient resources, including an adequate number of qualified staff, IT systems that allow the audit performance in an efficient and adequate way, according to the audit program planned for the reporting year. Will be assessed if the internal auditors benefit from continuous training and professional development in order to deal with the increasing technical complexity of the banks' activities and the increasing tasks diversity that should be performed as a result of introduction of the new products and processes in banks and other evolutions within the financial sector.

In order to verify if the audit function covers all the activities and risks to which the bank is exposed, will be assessed if the bank elaborates and implements at least annually the internal audit program and if it is approved by the bank's council. The frequency of the audit of activities and risks

(audit cycle) should be defined depending on the impact of the audited activity on the risk profile of the bank on the importance of this activity in the income obtaining.

The supervisor will assess if the internal audit function ensures the current reporting of the significant findings to the bank's council and the audit committee and informs the executive body. Also, will be verified if the internal audit reports quarterly to the bank's council and the audit committee about the results of the internal audit activity. The report should contain information about the achievement of the objectives/responsibilities, the sufficiency of the staff engaged in the internal audit process, the identified shortcomings, corrective measures and the results of monitoring the fulfillment of internal audit recommendations.

4.2. Risk management function

The bank shall have the risk management function under the direct supervision and responsibility of the council of the bank. It has the task to identify, measure, evaluate and monitor the risks to which the bank is exposed, to determine the capital and liquidity needs in the context of risks to which the bank is exposed, to monitor and assess the consequences of accepting certain risks, etc.

The supervisor should assess if the risk management function realizes at least the following:

1) identifies the risks to which the bank is exposed, measures, evaluates and monitors these risks and the real exposure of the bank to that risks

2) determines the capital and liquidity position in the context of risks to which the bank is exposed

3) monitors and assesses the consequences of accepting certain risks, mitigating their impact and matching the level of risk to the level of risk tolerance

4) reports to the bank's management body and issues relevant recommendations.

The supervisor should determine if the bank has a member in the executive body with general responsibility for the risk management function (Chief Risk Officer (CRO)). The CRO has the main responsibility of the supervision of the development and implementation of the risk management function within the bank. CRO is responsible for giving support the bank's council in its engagement to supervise the elaboration of the risk appetite and of the report on the risk appetite and for transposing of the risk appetite in a structure of risk limits. The CRO together with the executive body should actively involve in the performance monitoring in relation to risk taking and adherence to risk limits.

An adequate risk management requires the bank to dispose reliable risk management instruments based on reliable data sources. The risk supervision should be an integral part of the bank's culture and values. The risk dimension should be taken into account in a clear way in all the processes and development strategies of the bank.

When evaluating the risk management function, the supervisor will take into account that a sound risk culture set up at the bank level represents one of the key elements of efficient risk

management. Implementation of the adequate standards for a professional and responsible behavior in the whole bank should contribute to the reduction of the risk to which the bank is exposed.

The supervisor will assess if the risk management function permanently cooperates with the council and its specialized committees, mainly with the Risk Management Committee, for taking adequate decisions concerning the risk exposure of the bank. The risk management function reports that include identification of the new risks or of the existing risks that are not administrated, should lead at an adequate review of the internal controls and of the measures of diminishing of those risks.

4.3. Compliance function

The compliance function is an independent function within the bank, under the direct supervision and responsibility of the council of the bank that has the task to ensure the compliance of the bank's activity with the legal framework and internal regulations and to provide information regarding the evolutions in this field.

The supervisor will assess if the compliance function carries out its activity based on a program that includes, at least:

1) implementation and review of specific policies and procedures

2) assessing the compliance risk, testing and informing the bank's staff on the compliance aspects

3) verifying the compliance of the new products and new procedures to the legal framework and its amendments

4) elaboration and appliance of the methodologies of evaluation the compliance risk by using the performance indicators

5) monitoring and testing the compliance based on relevant tests and communication of results according to the reporting lines of the bank and to the internal risk management procedures.

A banking management framework that works according to the bylaws, internal regulations of the bank and the legal framework in an indicator of efficient functioning of the compliance function within the bank.

The supervisor will assess if the compliance function staff:

1) has access to any records, information or documents necessary for fulfillment of the tasks and responsibilities

2) can conduct investigations on the possible violations of the compliance policy and reveals freely the findings to the management body

3) proposes recommendations for the purpose of correction of the identified non-compliance situations.

The supervisor will assess if the composition and the structure of the compliance function are according to the nature, size and the complexity of the activity performed by the bank. In this regard, will be analyzed the organization of the compliance function at the banks with a similar risk profile.

Within the limits of available information sources will be assessed if the compliance function participates at the approval of the new products or at the significant changes brought to the existing products, processes and systems. The role of the compliance function consists in assessing the compliance of the rules of application of new products with the applicable legislation, especially in the process of marketing and communication of the new products and services.

The report of activity of the compliance function should contain information about the activities of the compliance function performed in the reporting period (for example: the result of risk compliance evaluation), the significant changes in the legislation in force, the identified compliance deficiencies and recommendations for their remedial, etc. This report should be well documented and presented at least annually to the management bodies.

5. Risk management framework and risk culture

The analysis of the risk management framework concentrates on 3 key dimensions:

1) Risk Appetite Framework
2) Risk culture
3) ICAAP framework

These dimensions reflect the quality of the existing procedures and offers a support for the management body in the establishment and communication of the risk appetite and internal governance framework of the bank. For the evaluation of the internal governance framework of the bank, the important information sources are information obtained as a result of the dialog between the supervisor and the bank. This communication gives the supervisor a general image of the bank's risk level, because, as a rule, if the banks have a very open communication strategy, this is an indicator of a good risk profile management at the bank level.

5.1. The Risk Appetite Framework (RAF)

The supervisor should assess the bank's risk appetite through the risk appetite management framework and the risk limits, concentrating in the same time on the capacity to evaluate the real risk profile of the bank to the desired one. As well, will be assessed if the bank takes into account and applies RAF in the strategic decisional process at the level of the whole bank.

Implementation of an efficient RAF that will cover the activity of all the bank requires that it contains a combination of polices, processes, controls, systems and procedures at the bank level. At the RAF assessment, the supervisor will take into account these elements and will analyze the level of integration of the RAF in the decision making process and in risk management at the whole bank level.

The supervisor will assess the RAF quality including the discussions with the management body, as a result of assessment of the connection between the bank's business strategy and its risk

appetite, as well as following the results of the evaluation of the risk appetite impact on the bank's decisions.

The declaration regarding the risk appetite is a part of the bank's strategy and identifies the risks that can materialize in normal conditions and stressed conditions and establishes clear actions that are going to be taken for the reduction of these risks. It should include quantitative methods of risk quantification that can be easily associated and attributed to different business lines, branches and bank's subdivisions.

5.2. The risk culture

The management body of the bank should develop and promote high ethical and professional standards, taking into account the needs and the specific characteristics of the bank and to ensure the implementation of such standards. The applied standards should have as a goal the reduction of the risks to which the bank is exposed, and the management body is responsible for the supervision of compliance with these standards by the employees. Within the implementation of these standards, the management body must have clear and documented policies that will promote the risk awareness by a risk culture, with the reflection of its expectations, according to which the bank's activities will not exceed the risk appetite and the risk limits established at the bank level.

The supervisor will assess if the bank has implemented a risk culture at the level of each subdivision and not only at the level of specialists in the fields of risk or risk management, compliance and internal audit function.

Within the risk culture, assessment will be also analyzed if the bank's management body allocate sufficient time for the examination of the problems linked with the risk administration. This aspect will be assessed by the analysis of the management body minutes, decisions liked with the risk administration, the approved policies and the level of staff training.

The supervisor should analyze if the bank's risk culture is adequate for the extent, complexity and the nature of its activity, as well as if it is based on reliable and clear values, that take into account the risk appetite of the bank.

5.3. The ICAAP framework

The assessment of the internal capital adequacy (ICAAP) allows the supervisor to determine if the bank's internal capital can cover all the risks to which the bank is or can be exposed, in an appropriate manner to the nature and the level of these risks.

The supervisor will review the ICAAP process and determine its soundness, effectiveness and comprehensiveness, as well as will evaluate how the ICAAP process is integrated into general risk management and strategic management practices, including capital planning. The results of these evaluations will contribute to the calculation of the additional capital requirements.

For an overall understanding and validation of the bank's results related to ICAAP quantifications and their reliability, the results will be compared and reconciled with the quantifications made by the supervisor, and in case of recording differences between results, the supervisor will verify and identify the causes of these deviations.

When assessing ICAAP, the supervisor will take into account the results of internal governance assessment, control functions, administration, as internal capital estimations cannot be considered adequate without adequate governance and control mechanisms.

6. Conclusions

Trust in the reliability of the financial system is very important for its proper functioning. Sound internal governance arrangements are fundamental for a good functioning of the banking institutions individually and the banking sector as a whole. Ensuring an adequate internal governance of the bank involves the correct establishment of the bank's strategic objectives, ensuring an efficient management of the bank's activity and internal control mechanisms as well as prudent administration of the bank's activity in accordance with the administrative, legal and prudential requirements and regulations. The internal governance should be appropriate to the nature, scale and complexity of the institution. The main responsibility for internal governance lies with the management body, which is subject to specific suitability requirements.

The areas that banks should prioritize in order to increase the quality of their internal governance are:

- proper functioning of the management body, including members' sufficient level of commitment and independence and establishment of adequate internal administration practices and procedures;

- developing a strong risk appetite framework, taking into account all the significant risks to which the bank is exposed, including risk limits, tolerances and thresholds;

- developing a solid and effective ICAAP process, to evaluate and maintain an adequate level of capital to cover the risks to which the banks are exposed or likely to be exposed;

- focusing on data quality, high quality data being a pre-requisite for effective control, and the basis of all sound decision making.

In the context of the mentioned above facts, the safety and viability of banks is crucial to their financial stability, and their efficiency is directly proportional to the way their activity is managed. A poor governance of banks can result in the extension of their problems to the level of the banking system, thus violating both the rights of shareholders and of the depositors, being endangered the financial soundness of an economy.

Assessment of the internal governance during the Supervisory Review and Evaluation Process and informing the banks about all the identified shortcomings will improve their internal governance.

Effective internal governance plays a key role in ensuring the continuity and stability of the bank. A permanent and timely assurance of the capital adequacy, liquidity, profitability and asset quality, an efficient management of the banking activity, the compliance with laws and internal policies, represent a guarantee of a successful banking business and creates prerequisites for a sustainable development of banks.

References

European Banking Authority (2014), *Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP)*, retrieved from https://eba.europa.eu.

European Banking Authority (2017), *Report on guidelines on internal governance*, final, retrieved from https://eba.europa.eu.

Khan, H. (2011), A Literature Review of Corporate Governance, *International Conference on E-business, Management and Economics IPEDR, Vol.25 IACSIT Press, Singapore*, pp. 1- 5.

KPMG (2018), *Internal governance: Addressing weaknesses*, retrieved from https://home.kpmg/xx/en/home/insights/2018/06/internal-governance-addressing-weaknesses-fs.html.

Naciri, A. (2009), *Internal and External Aspects of Corporate Governance*, London: Routledge.

Roman, A. (2019), *The Three Pillars of Corporate Governance*, retrieved from https://www.azeusconvene.com/articles/three-pillars-of-corporate-governance.

Assessing the Risk of Fraud in the Internal Audit Mission

Inga BULAT*, Rodica PERCIUN*

Abstract

The purpose of an internal audit is to provide advice and provide objective assurance on the effectiveness of the managerial internal control system by providing recommendations that ensure and contribute to improving the work of the public entity. By assessing systems, processes, high-risk activities in the presence of errors, fraud, irregularities or significant non-conformities. The reality shows that, depending on the determinants, synthesized in pressures, opportunities and attitudes, there are significant differences in the risk of fraud. Differences can be identified at different levels of the internal control system, areas of activity and in different times, between financial years. The risk of fraud and corruption must be managed by the entity's management but also regularly evaluated by the internal auditor in conducting audit engagements. The establishment, assessment of the control environment and the management of major risks with a high degree of fraud implies a concise mechanism of effective activities in the prevention of fraud and corruption at entity and process level. This article will outline the basics of fraud in the public entity, the assessment of fraud risk by internal auditors using non-statistical models and indicators.

Keywords: internal audit, fraud risk, internal control, fraud, audit mission, entity.

JEL classification: H83, G32, M42, C33.

1. Introduction

The achievement of the managerial internal control process within the public entity ensures the optimal management of the resources according to the objectives of the public entity, based on the principles of good governance that are ensured through policies, procedures and the approach of associated risks. Effectively implemented rigorous control systems can significantly reduce the risk of fraud but cannot completely eliminate the risk of fraud occurring or remaining undetected. From the perspective of the concept of "fraud" we can define: data from several sources, such as:

- an illegal act characterized by the deceit, deception or betrayal of trust committed by a person or a public entity for the purpose of obtaining funds, goods / values or services, or evading payment, in order to secure a personal advantage in business, and "error" is defined as the irregularity of violation of the regulatory environment and relevant internal regulations of the public entity,

* Ph.D., National Institute for Economic Research of Moldova; Email: bulat.inga124@gmail.com
* PhD Hab, associate professor, National Institute for Economic Research of Moldova; Email: rodica21@gmail.com

consisting of an unintentional activity or omission which adversely affects or may adversely affect the activity of the public entity (The Law on Prevention and Combating Corruption)

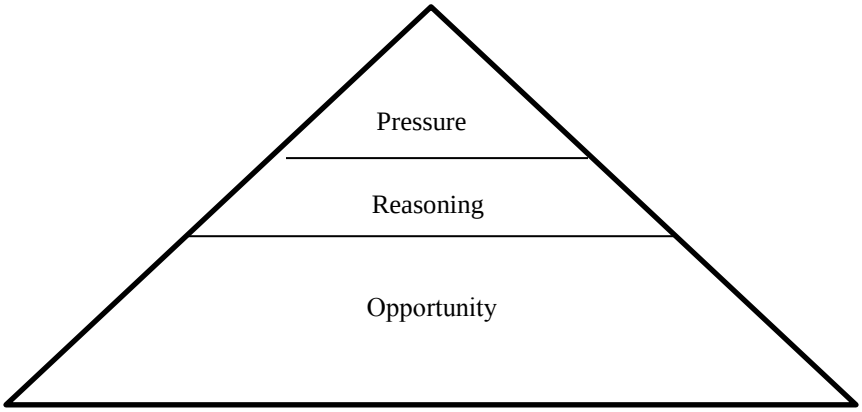
- intentional and hidden actions committed both by parties / individuals inside and outside the entity. Actions are illegal and denote illegalities. The shares result in loss of funds of its entity, its value and reputation, any other illegal advantage obtained personally or by other parties. (Law on Prevention and Combating Corruption, 2008)

- distortions of financial statements that may result from fraud. The factor that distinguishes "fraud" is the extent to which the action behind the distortion of financial statements is intentional. (Wikipedia, 2019)

There are two types of intentional misstatements that are relevant to the auditor - misstatements resulting from fraudulent financial reporting and misstatements resulting from the misappropriation of assets. Although the auditor may suspect or, more rarely, identify fraud, the auditor does not make any legal determination as to whether the fraud really took place. (International Regulations on Quality Control, Auditing, Review, 2015, p. 168)

Persons who commit fraud take advantage of weak internal controls or the possibility of neglecting controls and are motivated by the desire to obtain money or other unfair advantages.

Figure 1. The basic characteristics of fraud identified on the basis of the "triangle of fraud"



Source: Vona L.W. Fraud risk Assessment: Building a fraud audit program Hoboken: NJ, John Wiley & Sons 2008, p. 7

1. ***Opportunity*** - person who has access to the activity or manages a control procedure that allows for system fraud. The position of a person, as well as his responsibilities and authorization, also contribute to the possibility of committing fraud.

2. ***Reasoning*** - a conscious decision of the perpetrator to place his needs above the needs of others. Ethical decision-making varies depending on person, culture, and experience.

3. ***Pressure*** - are events taking place within the entity or in the individual's life. Pressures vary according to the global risk factor.

Six premises must be understood by applying the triangle of fraud concepts:

1. The three elements of fraud - rationalization, pressure and opportunity - coexist at different levels on the entity's staff.
2. Fraud elements will vary according to your personal circumstances.
3. The power of an element can cause a person to commit a fraudulent act.
4. Resistance of an element can eliminate the concern.
5. Identifying the three elements is easier than measuring the three elements.
6. Fraud risk factors may come from internal or external sources.

The three elements of fraud co-exist at different levels within the organization and influence each individual differently.

The power of one can cause a fraudulent or a combination of elements.

Perhaps the power of an element can eliminate fear of the perpetrator's detection. Therefore, the fraud assessment process must take account of fraud

From the above, one can conclude that there are various processes of fraud in an entity's internal control system. The most important is the decision-making culture in establishing internal procedures for assessing the vulnerability of the internal control environment through effective tools to identify, manage and report fraud risks.

2. Internal audit responsibility for fraud risk assessment in audit engagements

In fact, identifying the condition of fraud is easier than measuring the items. The audit process should be aware of the condition of fraud, but the classification of the three factors is extremely subjective. The auditor's response to the assessed risks of a process or whole system is based on evidence that it does not contain material misstatement due to fraud or error. Due to the inherent limitations of an audit, there is an inevitable risk that some significant misstatements in the process or system will not be detected even if the audit is planned and performed in accordance with ISAs.

In the internal audit engagement, the purpose of the auditor is to establish the objectives that take into account the probability of significant errors, fraud, nonconformities and other risks (SNAI 2210), and in order to support his opinion, the auditor needs to obtain a number of sufficient evidence appropriate and to assess the influence of the risk of fraud on the distortion of the information presented in the documents analyzed. Expressing an opinion of the evidence obtained on the distortions is objective, independent and professional in accordance with the regulatory framework, which ensures the suspicions obtained under the most significant aspects.

Therefore, internal auditors have sufficient knowledge to assess the risk of fraud and how it is managed by the public entity by assessing the possibility of committing fraud acts and how the public entity manages the risk of fraud. (Law, Public internal financial control, 2010)

Through reasonable assurance engagements, reasonable assurance is given that the internal control system, as a whole, does not contain material misstatement as a result of fraud or error. By

objectives set at:

- the planning stage, the internal auditor identifies and assesses the risks of material misstatement of the internal control system and financial statements as a result of fraud;

- the execution stage, the internal auditors obtain sufficient and appropriate audit evidence about the assessed risks.

The auditor should apply a series of procedures to test the existence or absence of fraud risk at the level of the audited entity or process, depending on a range of financial and non-financial factors. According to the International Standard of Auditing (ISA) 240, the auditor should maintain professional skepticism throughout the audit, recognizing the possibility that material misstatement as a result of fraud may exist by disregarding the auditor's experience of honesty and integrity of management and responsible persons with the governance of the entity. (International Audit Standard, 2015, p. 168)

The skepticism and professionalism of the auditor to identify possible fraud opportunities depends on the techniques and tools used in the audit engagement. The auditor's risk is more difficult to detect significant misstatement as a result of management fraud than employee fraud, given that management is frequently in a position to manipulate directly or indirectly. Thus, the auditor will have to show professional skepticism throughout the audit, to obtain reasonable assurance, to take into account the possibility for management to avoid controls and to recognize that audit procedures that are effective for detecting errors may not or effective for detecting fraud. The internal auditor should use procedures to detect such misstatements in identifying and assessing the risks of fraud.

An auditor conducting an audit in accordance with ISA will obtain reasonable assurance about misstatements by applying ISA 315, Identifying and Assessing Risks of Material Misstatement by Understanding Entity and its Environment and ISA 330.

The internal auditor must have sufficient knowledge to assess the risk of fraud and how it is managed by the public entity by assessing the possibility of fraudulent acts and how the public entity manages the risk of fraud. (Law, Public internal financial control, 2010) The role of fraud detection audit, which is not the most important, is to analyze and test control tools.

Through reasonable assurance engagements, reasonable assurance will be given that the internal control system as a whole does not contain material misstatement as a result of fraud or error, thus contributing to the prevention or detection of subsequent fraud. (Table 1).

As outlined in ISA 240, the potential effects of inherent limitations are particularly important in the case of fraud resulting from fraud. The risk of not detecting significant misstatement as a result of fraud is greater than the risk of not detecting a misstatement resulting from the error. This is because fraud may involve sophisticated and carefully organized schemes designed to conceal, such as forgery, deliberate failure to record transactions, or intentional misrepresentation auditor addressed. (International Regulations on Quality Control, Auditing, Review, 2015, p. 70)

Table 1. Potential contributions by the internal auditor to prevent or detect fraud.

Mission type	Prevention of fraud	Detection of fraud	Auditors role
Assurance mission	1. Identify and evaluate all internal and external risks that could lead to fraud; 2. testing existing anti-fraud measures; 3. Creating a list of fraudulent practices detected in audits they have carried out to raise awareness of fraud.	1. Establishment of fraud indicators. 2. Methods and models for assessing fraud risks; 3. Analysis of internal documents and sensitive posts.	1. formulating recommendations for improving the internal regulatory framework in place to prevent fraud; 2. Reporting weaknesses or deficiencies; 3. formulating appropriate recommendations or corrective measures for management to avoid future fraud; 4. Reporting the weaknesses of the deficiencies and the vulnerability of the internal control environment.
Counseling mission	1. Participating in the establishment of a national anti-fraud strategy within the entity by sharing their experience; 2. formulating recommendations for improving the internal normative acts in force; 3. advising on planned activities to identify corruption / fraud based on prior knowledge and experience.	1. Establishment of fraud indicators. 2. Analysis of internal documents and sensitive posts.	1. Reporting weaknesses or shortcomings to the competent authority, without delay or at least as soon as possible; 2. where appropriate, formulating recommendations to avoid future fraud; 3. formulating appropriate recommendations or corrective measures for management

Source: *elaborated by the author*

Discrimination can be more difficult to detect when accompanied by complicity and a well-thought-out scheme in the application of the corrupt scheme.

Thus, the risk assessment of fraud will be done through the analysis of the vulnerability of the internal control environment to the management and reporting of financial resources as follows.

- in the case of expenditure - a deliberate act or omission involving:

(i) the use or submission of false or incorrect or incomplete statements or documents that has the effect of misappropriating or illegally holding funds from the public budget,

(ii) failure to disclose information that violates a specific obligation having the same effect

(iii) misappropriation of such funds for purposes other than those for which they were originally granted.

- Income - A deliberate act or omission involving:

(i) the use or disclosure of false or incorrect or incomplete statements or documents which has

the effect of illicitly diminishing public resources,

(ii) failure to disclose information that violates a specific obligation having the same effect

(iii) misappropriation of a legally obtained benefit having the same effect.

An analysis of the risks of distortion and fraud will be made at:

- planning stage - identifying and assessing the risks of material misstatement of the internal control system and management of financial resources;

- the execution stage, the auditors are to obtain sufficient and appropriate audit evidence about the assessed risks.

The procedures applicable by auditors at different stages of the audit engagement to identify / determine the risk of fraud / corruption are:

- stage of knowledge process / activity, auditors will examine the process of identifying and managing the risks of fraud / corruption and if the existing internal control system, prevent and / or detect such risks.

- Identifying the factors leading to the risk of fraud is to accumulate information on the internal control system and analysis of performance measures of the public entity in the last few years to identify the presence of models inconsistent; this will identify weaknesses in the internal control that creates premises for fraud

- fraud / corruption risk assessment for auditors is an instrument for determining the probability of committing fraud / corruption and the consequences for the public entity when it / they will occur. Therefore, the fraud triangle is a component that also provides for risk assessment within the internal audit engagement, and when assessing the fraud risk factor, auditors should consider:

- the correlation between the opportunity to commit fraud and the ability to hide,

- ability and issues that affect employees,

- culture and ethics of the organization in decision-making and internal control.

During their internal audit described the evidence that can be considered as suspected fraud and the possibility of fraudulent financial reporting, based on indicators that may indicate possible risks of fraud / corruption that can be called "red flags" or "strong warning" and requiring immediate attention to detect possible fraud / corruption cases.

Indicators that may indicate possible fraud / corruption risks at the public entity level, such as: (Decision of CC RM, 2016)

- fraud indicators in financial reports;

- indicators of forged documents;

- Indicators in the field of contracting and procurement;

- assets ratios;

- indicators for corrupt payments;

- Indicators of conflicts of interest, etc.

Another classification of the indicators is in the Methodological Standards of Public Internal Audit establishes indicators such as:

A. Opportunity / circumstances:

- the type of public entity or subdivision
- complex organizational structures or permanent change
- inefficient driving control
- insufficient internal control
- Differences in financial transaction management
- lack of evidence or contradictory evidence

B. Rationale / justification

- neglecting the risks
- strange or deviant behavior

C. Performance and pressure incentives

- personal financial pressure on management and employees
- unfavorable relationships.

The internal audit activity must always comply with the relevant legislation, standards and instructions accepted at national and international level. By setting the limits of its competencies and its obligations towards the manager of the public entity and the foreign bodies. An auditor should be objective in clear and relevant evidence in identifying potential indications of suspicion of fraud and corruption.

The role of the auditor in detecting a potential fraud case is limited to detecting and recording suspicious circumstances, based on the facts established by the audit, including on-the-spot checks. Auditors should report / inform the hierarchically superior manager, the manager of the public entity or, as appropriate, the competent law enforcement authorities in writing of suspicious circumstances. This stage offers the possibility to carry out in-depth verifications or on-the-spot checks or involve other authorities, as the case may be. At the end of the process, the internal auditor will have to be able to reasonably decide whether or not there was an irregularity and, if so, to determine the financial remedies to be applied. They should also be able to decide whether a case should be referred to the judicial authorities and whether it is necessary to inform the manager of the public entity.

3. Models for risk assessment of fraud through statistical procedures.

When sufficient evidence is obtained, the internal audit will use models based on the estimation of the survival function, such as the *Kaplan-Meier* estimator (Vona, 2008), also known as the product and / or service limit estimator and the *Cox model*.

Kaplan-Meier's estimator will estimate the survival function of the entity subject to financial fraud, processes, field of activity, and levels of financial leverage, and the Cox model will estimate the gambling function of processes that are subject to financial fraud (fraud risk assessment).

The combination of estimation and testing of the hazard function coefficients is achieved by

predictive factors (entity's scope of activity and leverage levels).

It is a nonparametric statistic used to assess the risk of fraud. By the survival function ***S (t***) it is probable that a process or transaction will survive the moment ***t, i_e*** the probability that the fraud did not occur until the time ***t***: (Statistical Fraud Risk Assessment, 2014, p. 22)

$$S(t) = P(T > t) = 1 - F(t) = \int_t^{\infty} f(x)dx \quad (1.1)$$

By the Kaplan-Meier estimator, $S_{(ti)}$ at different time points, t_i can be defined as:

$$\hat{S}(t_i) = \prod_{t_{i-1} \le t_i} (1 - \hat{m}_i) \quad (1.2)$$

where is the likelihood of knowing the fraud at the time of you ***t***, and $(1-m_i)$ is the probability of not knowing the fraud. Graph by survival survival *curve graphically*.

In order to compare the probability of not subjecting the processes to fraud according to the object of activity and the level of the leverage, the functions / survival elements of the selected samples will be compared. Differences between them will be tested using the Log-Rank test statistic.

The Log-Rank test is:

$$U = \sum_i (O_i - E_i) \quad (1.3)$$

where: **Oi** – - the number of processes / transactions (fraud) observed

Ei – the number of processes / transactions (fraud) estimated.

For the acceptance / rejection of the survival function matching assumption for the studied groups the calculated value of the Log-Rank test is compared with the theoretical value of the ***Hi square*** with ***(k-1)*** degrees of freedom, where k is the number of samples.

The COX model estimates and tests the influence of the field of activity and the level of leverage on the risk of fraud. [10]

The Cox model allows the analysis of long-term data, similar to regression models. The Cox model estimates the hazard rate, h (t), knowing the event studied by a linear combination of p explanatory factors $(X_1, X_2, ..., Xp)$.

The hazard rate can be defined in the form of:

$$h(t) = [h_0(t)]e^{b_0 + b_1X_1 + ... + b_pX_p} \quad (1.4)$$

or in logarithmic form

$$\ln h(t) = \ln h_0(t) + b_0 + b_1X_1 + ... + b_pX_p \quad (1.5)$$

where $h_0(t)$ represents the reference hazard rate, and bi is the regression coefficient.

The rate of risk that the sample population contains fraudulent items during the observed

period, under the influence of preachers (field of activity and financial leverage) can be estimated using a SPSS program. (Statistical Fraud Risk Assessment, 2014, p. 24)

The final elements that conclude certain processes concern the hazard rate values at different time points, the regression coefficients associated with the preachers, and the degree of their statistical significance.

The coefficients of regression are also calculated as exponential (eb, where "***e***" is the basis of the natural logarithm).

The percentage change in the hazard rate, with a change of 1 unit of the predictor variable, is equal to ***100 (eb -1)%.***

Testing the significance of regression coefficients is based on the Wald test statistic and is calculated as follows:

$$Wald = \frac{b_j^2}{\hat{\sigma}^2_{\hat{\beta}_j}} \quad (1.6)$$

Where: ***bj*** represents the value of the regression coefficient, and the standard deviation of the parameter estimator ***βj***.

Based on the Kaplan-Meier estimator and Cox model function, the time elapsed between the start of the first reporting and the occurrence of the fraud, the status of the entity at the end of the analyzed period (fraudulent / unframed), the scope of activity and the financial leverage.

4. Conclusion

The primary responsibility for preventing and detecting fraud lies with the Managing Authorities. However, the success of the fight against fraud depends on the joint efforts of managing authorities, the internal auditor and other stakeholders. Each participant in the chain must fulfill its role in protecting the financial interests of the public entity.

Internal auditors can play an important role in preventing and detecting fraud at different levels. In most cases, the recommendations made by internal auditors to strengthen management and control systems will also have a positive impact on the prevention of fraud.

The main contributions to preventing and detecting fraud, those internal auditors can make by conducting audit missions in the field of financial resource management and internal control environment.

References:

Aren J., Loebbecke Al., (2003) Audit: An Integrated Approach, ARC Publishing House, Translated by Rodica Levitchi - Auditing: An Integrated Approach, 8th Editions, published by Pearson Hall.

Dobroţeanu L., Dobroţeanu C. L., (2002) Audit. Concepts and practices. National and International Approach, Ed. Economică, Bucharest.

Ghiţă, M., Pereş I., Bunget, O., etc., (2005) Public Internal Audit. Concepts and Methodology, Mirton Publishing House, Timişoara.

Vona L.W. (2008) Fraud Risk Assessment: Building a fraud audit program Hoboken: NJ, John Wiley & Sons.

International Audit Standard nr. 240.

Law ”Prevention and Combating Corruption”, nr. 90-XVI of 25.04.2008.

Law”Public internal financial control” nr. 229 from 23.09.2010.

Decision of CC RM (nr. 8 of March 21, 2016) Approving the Regulation regarding the procedures applied within the Court of Accounts in the case of identification / determination by the auditors of the risk of fraud / corruption.

International Regulations on Quality Control, Auditing, Review (2015) Other Insurance Services and Related Services, Volume 20.

Statistical Fraud Risk Assessment for Audit Opinion Based on Durable Models (2014) Financial Audit nr. 4.

Economic Students' Perception of the English-taught Bachelor's Programme

Elena TĂLMĂCIAN*

Abstract

The present article is based on a research on economic students' comfort degree regarding the experience of being taught in English. The survey was addressed to 150 1st year students within The Faculty of Accounting and Management Information, the Bucharest University of Economic Studies that are taught the whole academic program (6 courses and 7 seminars) in English. Although most of the surveyed students have a C1 level of English, our target was to find out the challenges of an academic program in English, whether there are any communication barriers, how comfortable surveyed students feel about being taught in English, taking into account the fact that the subjects that they study are economic ones, therefore they operate with lots of specialized terms and expressions which may unfavorably impact students' comprehension.
The present paper represents only a starting point for the research of this topic and our intention is to expand it and eventually approach it from the professors' perspective in order to get a comprehensive view of our research topic.

Key words: English-taught bachelor's programme, economic students' perception, comprehension challenges

1. Introduction

The English language can be called "the fastest-spreading language in human history" (Michaud, 2012) being "spoken at a useful level by some 1.75 billion people worldwide - that's one in every four of us." (Michaud, 2012) The issue of the ubiquitous spread of English can be found in the literature as well: Corcodel, Corcodel and Corcodel (2011, pp. 283-284) call English "the Latin of today", "the main language of international trade and commerce", "not only the language of contracts when one of their parties comes from an English-speaking environment but even when no native English-speaking party is involved" and such examples are numerous.

* Elena TĂLMĂCIAN is a university lecturer at the University of Economic Studies, Bucharest. E-mail: elena.talmacian@rei.ase.ro

So, while it is generally accepted that English is "the global language of business" (Neely, 2012), most people are fully aware of the advantages of the knowledge of this language both at an individual and economic level: "There is a general belief that success in English, beginning at the school level, is a key factor in national competitiveness and is of paramount importance to national economies in a globalized world." (Hayes, 2012, p. 47) This awareness is valid at the governmental level as well and governments "have, accordingly, made significant investments in programmes and projects designed to improve the teaching and learning of English in state schools across the age range." (Hayes, 2012, p. 47)

The questionnaire included in Sandström & Neghina (2017, p. 9) research regarding English-taught bachelor's programmes (ETBs) in 19 European Higher Education Area (EHEA) countries including Romania revealed the fact that "according to the professionals interviewed, ETBs were a novelty a decade ago when they were introduced but have become a relatively common aspect of internationalisation with many institutions developing more ETBs as a response to increased demand and global competition."

It is a conviction that is transparent in the answers of the surveyed students as they all agree that the more economic English they know, the better for their future careers and not only. It is what a recent survey that was addressed to 16,344 employed adults in 26 countries like Sweden, Turkey, Great Britain, Spain, Canada and Italy concluded, namely "that people with higher levels of income or education were among the most likely to say English was most commonly used for foreign business relationships" (Michaud, 2012).

2. Research methodology

By means of the survey method we have tried to find out the students' perception of their exposure to a whole academic programme (6 courses (C) and 7 seminars (S)) in English. The survey was addressed to 150 1st year students within The Faculty of Accounting and Management Information, the Bucharest University of Economic Studies.

Although it is common for every university to have programmes taught only in English, there is a lack of research on students' feedback regarding such programmes from the linguistic point of view or of the English language challenges they face when they are, for example, first year economic students having to deal with subjects like Business Law in English or English for professional communication with foreign terms and expressions that may pose serious understanding problems.

3. Survey and findings

The survey is made up of seven questions by which the surveyed students have been able to offer their feedback regarding the English delivery of the courses and seminars of the academic programme they attend focusing on the challenges that it may pose.

The first question *"How many courses & seminars in English do you have? Please, list them"* serves as a starting point and is meant to show the wide variety of economic courses (C) and seminars (S): Business Law (C+S), Mathematics applied in Economics (C+S), Introduction to accounting (C+S), Management (C+S), Professional Office Applications (C+S), Microeconomics (C+S), English for professional communication (S).

According to the students' answers to the second question *"Do professors read or speak English freely? Both?"*, teachers in this programme speak both freely and read courses. Teachers focus on reading especially when they deal with definitions and sometimes "they use Romanian as well to express some terms or themselves better." Actually, the need to appeal to Romanian in absolutely natural, as: "equivalence in terms of complete identity would be impossible because languages are different and complex linguistic systems and translation takes place not only between languages but also between texts embedded in complex communicative situations." (Chifane, 2012, p. 81)

A typical answer to the third question *"Do you interact with Romanian teachers only in English? If you do not, why?"* is: "Most of the times we interact with professors in English. I am saying "most of the times" because sometimes it is hard to translate an exact meaning from Romanian to English." Also, "it happens to us not to know sometimes how to express a certain phrase in English at that moment." So, their avoidance to use English is generally caused by the lack of knowledge of a certain economic term or expression or by problematic translations, cases in which they get help from the teacher.

Most answers to the fourth question *"If you do not know certain terms or expressions, do you ask your teacher(s) to clarify them?"* revealed the fact that students prefer to google the meaning of unknown economic words or phrases as this way they can find the information they need quite easily "we try to find the meaning by ourselves since we can find it quickly on the internet" or some of them are too shy to ask the teacher for clarifications and get out of their comfort zone: "I do ask them about unknown terms, but not all the time, I am too shy to do that".

Our respondents' answers to the fifth question *"What challenges do you face regarding the English language during the courses (seminars) taught in English? (e.g. new economic expressions, misunderstanding of terms, teacher's stress/ fluency in English, etc.)"* brought to light some of the problems that they have encountered as speakers of English as a second language. Among these they have mentioned unknown economic English terminology (e.g. "new terms that I have to learn and accumulate fast in order to understand the lesson"), the teacher's speed pace (e.g. "sometimes some teachers speak too fast"), albeit very sporadically teachers's stress (e.g. "sometimes the pronunciation of some professors is hard to understand, but generally our teachers know good English, so understanding is not a problem"). In her paper, Radu (2014, p. 167) signaled the great responsibility of the teacher saying "it would be beneficial to analyze to what degree teachers using English as a medium of instruction perform their roles of facilitators in the educational process and promoters of an appropriate vocabulary and good use of English".

But the most problematic issue of all seems to be the misunderstanding of some words which trigger serious damage to correct understanding of the respective economic content:

- "A big problem is represented by word misunderstandings, and because of that sentences do not make sense […] or maybe my knowledge in some economic subjects (like Business Law) are too little.";
- "The specific terms of a field can be hard to understand at first, for example, accounting terms."
- "Some of us were not used to talk English on a daily basis, so it can be hard to keep it with the speed and the volume of economic information in English".

The sixth question *"Do you find courses/ seminars in English useful for your English language improvement? Please, explain."*

All respondents agreed on and even stressed the fact that English-taught subjects are of great help for their English language proficiency:

- "I do find courses/seminars in English useful for my English language improvement because of multiple reasons. First of all, by hearing and speaking English every day I get more accustomed to it and I become better at it. Secondly, I learn some terms in English that I might not have the occasion elsewhere.";
- "Yes, I do find courses in English important because I am learning to speak English better this way.";
- "I definitely think that they are useful for improving our English. Once we start practicing and listening to English more, we will get used to it and we will catch up in order to get the fluency of the language."

The surveyed students were also invited to provide other relevant comments or examples and through it we have discovered that the students that have chosen the university programme taught in English have a very strong motivation supporting their choice:

- "We think that English academic programmes are more beneficial to us than those in Romanian. English is a language required by most if not by all the big companies. The fact that we know another language helps us grow professionally and personally. Whether we are talking about applying to multinational companies or communicating with people from other cultures."

They also know they have not chosen the easy way, but they know for sure it is the better way:

- "Even if it is harder, I consider that nowadays you have an extraordinary big advantage over someone who does not know English, in your professional life, but also in your social one."

Moreover, there is a certain enthusiasm about studying in English, be it economic English: "I really like to learn in English!". Therefore, students learn it with pleasure, they are perfectly aware that studying economic subjects in a foreign language (even if their exposure to English is considerable) is a more difficult road to follow than studying them in their native tongue, but they also know that their efforts are not in vain. On the contrary, they will have a huge advantage on the

job market and not only: "I need to actually learn new words that will be very useful in the long run and courses like Accounting and Business Law are courses that considerably enrich our economic vocabulary."

4. Final remarks

By means of the survey method some of our expectations supported by our direct teacher-student relationship experience were met. Absolutely all surveyed students agreed on the high importance of the (economic) English knowledge especially for their future careers and welcome the fact that all the subjects are taught in English giving them a feeling of security regarding their future and of certainty that they have made the right choice by enrolling in the respective bachelor's programme.

Still, there are some challenges that they strive to overcome and the most common challenge seems to be the difficulty of the economic terms that inherently pose understanding problems or determine sometimes the feeling that they cannot keep up with the quantity of new economic knowledge in a foreign language (English). But all these challenges are perceived by them as being part of their preparation for their future careers and even personal development.

Appendix: Survey

1. How many courses & seminars in English do you have? Please, list them.
2. Do teachers read or speak English freely? Both?
3. Do you interact with Romanian teachers only in English? If you do not, why?
4. If you do not know certain terms or expressions, do you ask your teacher(s) to clarify them?
5. What challenges do you face regarding the English language during the courses (seminars) taught in English? e.g. new economic expressions, misunderstanding of terms, teacher's stress/ fluency in English, etc.)
6. Do you find courses/ seminars in English helpful for your English language improvement? Please, explain.
7. Other relevant comments/ examples

References

Chifane, C. (2012). Equivalence versus non-equivalence in economic translation, *Management Strategies Journal*, *Vol. 18*, issue 4, pp. 74-82.

Corcodel, S., Corcodel, A., Corcodel, D. (2011). Equivalence in translating economic terminology (Incoterms), *Buletin ştiinţific, La formation en terminologie*, nr. 8, Bucharest, pp. 276-290.

Hayes, D. (2012). Planning for success Culture, engagement and power in English language education innovation, Issues in ELT change management, *Managing Change in English Language Teaching Lessons from experience*, London, pp. 47-60.

Michaud, C. (2012), English the preferred language for world business: poll. Retrieved November 14, from http://www.reuters.com/article/us-language/english-the-preferred-language-for-world-business-poll-idUSBRE84F0OK20120516

Neeley, T. (2012). Global Business Speaks English in *Business Harvard Review*, *May 2012 Issue*. Retrieved October 12, 2019 from https://hbr.org/2012/05/global-business-speaks-english

Radu, C. (2014). Teaching and Learning Business in a Foreign Language – Challenges and Opportunities, *Studii de diversitate culturală și limbaje de specialitate*, Cluj-Napoca, pp. 166-182.

Sandström, A-M and Neghina, C. (2017). English-taught bachelor's programmes Internationalising European higher education, European Association for International Education, Amsterdam. Retrieved November 20, from https://www.studyportals.com/wp-content/uploads/2017/09/EAIE-StudyPortals-English-taught-bachelor-programmes-Europe.pdf

Acknowledgements

Our special thanks to the 150 1st year students enrolled in English-taught bachelor's programme within The Faculty of Accounting and Management Information, the Bucharest University of Economic Studies for agreeing to be surveyed.