THE IMPACT OF INFORMATION AND COMMUNICATION TECHNOLOGIES ON THE EFFECTIVENESS OF INTERNAL CONTROL SYSTEM IN BANKS

CARA ION, PhD Student
e-mail: ion.cara3@gmail.com

Academy of Economic Studies of Moldova
61 Banulescu Bodoni Street, 2005 Chisinau, Republic of Moldova
Web page: www.ase.md

Abstract. *Information and communication technologies are one of the most important factors in the efficient operation of the bank's internal control system. The development of new technologies and their inclusion in the information systems of banks, has predetermined the formation of cyber or information risks to which banks are exposed due to obsolete information systems. Therefore, the need to review and improve internal control systems in banks cannot be avoided. Based on the topic, the purpose of this study is to assess the role of information and communication technologies and their impact on the efficiency of the internal control system and its components (control environment, risk assessment, control activities, information and communication and monitoring activities) in banks. It also reflects the way in which information technology and electronic data processing influence banking processes. In this regard, the following research methods were used: analysis and synthesis, induction and deduction.*

Key words: *internal control, information and communication technologies, informational system, risk.*

JEL CLASIFICATION: G32, M40

INTRODUCTION

Banks are increasingly relying on digital processes in order to achieve competitive advantages in terms of operational efficiency, reducing costs and human errors but also to increase the speed of transaction processing. Nowadays, banks give more attention for information systems development that also involve computer technology and tend to integrate the dispersed processes into a single harmonious system that generates complex information to the bank's governing bodies to achieve a greater performance of their functions, including the internal control function. The role of information systems on the efficiency of internal control is reflected by their ability to: identify deviations from the bank's objectives and related decisions of the bank's management on operational activity, make necessary adjustments to the management process in a timely manner, taking into account changes in both internal and external environment and as well as the exercise of systematic control over the activity of the bank subdivisions. The implementation of the mentioned tasks contributes both to the consolidation of the control efficiency and to its centralization, thus increasing the management level of the bank as a whole.

Along with the development of information and communication technologies (ICT), some new risks have arisen and the digitalisation of financial services could reduce banks' resistance to both cybercrime and cyber disruptions. According to the regulation of the National Bank of Moldova (NBM) on minimum requirements for information and communication systems of banks, ICT risk is considered a subcategory of operational risk that includes risks posed by compromising the integrity, distortion and unavailability of data and/or information systems as well as the lack of ability to cope

with new technologies and change them in a timely manner and at a reasonable cost. In order to achieve business objectives, the bank needs accurate, adequate, relevant, available and secure information technology (IT) which in turn will have an impact on the development of automated information systems. Therefore, it is indisputable that internal control cannot be effective if its organization, content and procedures are not improved together with the development of technological support for banking activities.

A comprehensive IT governance framework that addresses all aspects of IT and integrates them all into global IT standards is the COBIT (Control Objectives for Information and Related Technology) standard, developed by ISACA (International Association of Computer Systems Auditors). COBIT provides the basis for the creation of both general reliability rules and a mechanism for monitoring the efficiency of the use of information systems. According to the standard, information must comply with the criteria of availability, credibility, confidentiality, efficiency and integrity; however, if an activity involves the application of information resources but the information criteria do not match, it represents an information risk. Therefore, COBIT allows the use of best practices in information technology control, process maturity and an adequate level of reliability and control in the use of information technology. The standard covers the following areas of IT activity: (1) planning and organization; (2) acquisition and implementation; (3) supply and support; (4) monitoring and evaluation. It helps entities maintain a balance between achieving benefits and optimizing risk levels and resource use [6].

1. THE IMPACT OF ICT ON INTERNAL CONTROL ELEMENTS

According to the document „Integrated Internal Control Framework" developed by the Treadway Commission Sponsorship Organizations Committee (COSO), internal control consists of five interdependent components where information and communication technologies have either a direct or an indirect impact on each component which consequently play a huge role for establishing an efficient internal control system, as follows:

1. Control environment represents the attitude towards internal control and control awareness established and maintained by management and employees of the entity. In the meanwhile, it influences the setting of the bank's strategy and objectives and the way in which risks are identified, assessed and managed. The control environment can be considered a foundation for other components of internal control, as the environment determines the extent to which the components interact effectively and ensures their discipline and structure.

Information technologies are involved in all control environment factors, being used to allow the sharing and updating of information and monitoring the employees' compliance with the code of conduct and policies, standards and procedures of the bank. Thus, the IT solutions used in this regard facilitate, among other things:

- employees' access to the bank's internal page (intranet) which could include information on the bank's values, code of conduct and their importance;
- access to related information, thus beeing eliminated the necessity to keep paper copies;
- e-learning opportunities;
- notification by supervisors to staff in order to perform tasks;
- automatic reminder of the staff in order to perform the necessary actions;
- audit track of activities [2].

As the organizational structure provides the framework for planning, execution, control and monitoring of the bank's activity, it is necessary to mention the importance of the segregation of controls of as for subdivision responsible for information systems as well as for user subdivisions. Thus, the subdivision responsible for informatic systems is not authorized to carry out transactions and its functions has to be separated at least into three categories:

a) Programming:

- System analysis - analyzes the user's environment and requirements, thus, as specific changes as well as the acquisition of a new system or the design of a new information system could be suggested for implementation;
- System programming - the responsibility of this function involves the implementation, modification and troubleshooting of programs;
- Application programming - this function is responsible for writing, testing and troubleshooting application programs following the needs identified during the system analysis;
- Database administration - maintaining and restricting access to the database;
- Data preparation - can be prepared by user departments;

b) Operational - responsible for day-to-day operations using ICT equipment, supervising operations on virtual workstations and providing assistance;

c) Storage - the data library keeps the removable data and maintains the system and program documentation [7].

Therefore, the information system (which also includes the automation of the banking system) is the most important element of the control environment.

2. Risk assessment - an effective risk management system allows the identification, analysis of risks as well as the establishment of actions that need to be taken and could prevent the achievement of the bank's objectives. Therefore, the executive body should take the necessary measures to prevent risks and ensure they are handled properly to achieve the bank's objectives [4]. The main challenge of recent economic trends is to identify the balance between risks, costs and values to get more results from banks using as few resources as possible. In this context, financial risk management should be done automatically or in specific cases using special applications, thus, the automation of risk management processes would significantly increase the efficiency of this process. Changes to computerized information systems and operations may increase the risk of incorrect financial reporting.

The most common financial risks that affect the volume, profitability, value and structure of the bank assets and liabilities, where ICT plays an important role, are:

a) Interest rate risk - due to IT solutions, banks have the opportunity to simulate their activity using mathematical programming methods which allows the establishment of limits for the established parameters;

b) Credit risk - IT solutions represent an important resource in assessing the counterparties' creditworthiness, being used an internal rating system, however during the lending process is being used a scoring system for the borrower analysis;

c) Liquidity risk - information technologies allow real-time monitoring of structural fluctuations in assets and liabilities as well as the sensitivity of assets and liabilities to changes in interest rates and future capital requirements of banks;

d) Price risk - for the analysis of the risk of losses incurred due to changes in quotations for the bank's financial instruments, are required data on transactions and account balances, updated market rates as well as market indices. IT solutions allow the improvement of the systems used for analyzing

e-ISBN 978-9975-155-03-8

financial instruments (revaluation of securities portfolios at current market prices, performing calculations) as for monitoring compliance with existing requirements well as for reporting process;

e) Currency risk - in order to reduce the losses caused by exchange rate fluctuations, are used adecvate information systems that allow the real-time display of the exchange rates direction and information related to the international foreign exchange market;

f) Market risk - IT solutions allow the analysis of the uncertainty on the financial markets' situation development through various methods, such as calculating Value-at-Risk, Monte Carlo, sensitivity analysis of the portfolio to changes in market parameters, etc.;

g) Investment risk - the risk associated with the bank's investment activities can be analyzed by simulating investment processes, using appropriate software [8, 9].

In the Republic of Moldova, banks also use various information programs and software both in order to reflect the results of the control and to identify the reasons for risk exposure of their activity.

3. Control activities - are the policies and procedures that contribute to ensuring compliance with management directives and the actions needed to be taken to address the risks to the entity's objectives. As banks use information systems in order to manage their activity, to report, to follow changes in legislation but also to avoid potential losses, it was necessary to introduce control procedures on the electronic information systems used to perform these functions. At the execution level, depending on the technical support involved, control activities can also be automated and manual [2]. Control procedures for information processing are performed to verify the accuracy, completeness and authorization of operations, and information systems should include both general and specific controls:

a) general control refers to all aspects of IT systems within banks designed to ensure the integrity, accuracy and credibility of data and IT applications. Thus, in the event of weaknesses in the overall control, it may be unnecessary to review or evaluate the control of applications. There are many levels of general control, starting with the bank's management, which must ensure that IT is well managed and is responsible for setting the policy for the use of information technology within the bank. At the same time, the general control refers to the development standards and updating of new programs and systems within the bank, control of access to programs and data, control of computerized operations, IT security procedures, rules for installing applications on workstations, back up and restoring information in the event of unforeseen events, etc.);

b) the control activities (specific) of the computerized applications are embedded in the IT application, involve the processing of individual operations and depend on the way the given application was programmed. Thus, applications automatically control data entry and ensure that supported applications are available and interface errors are quickly detected [1].

Automated systems used in information processing could generate more risks due to transaction processing, undetected errors, registration of infrequent operations, failure of technical or software equipment components, etc. Thus, it is also necessary to involve manual control by verifying the data entered into the computer with the primary documents or other information to ensure that the scheduled aspects of the financial reporting system and control activities have worked efficiently [7]. It is becoming obvious that the effectiveness of internal control depends largely on both the effectiveness of scheduled control activities that generate reports and manual monitoring activities. Otherwise, banks could generate data and software losses due to deficiencies in electronic equipment, systems and security as well as data recovery procedures.

e-ISBN 978-9975-155-03-8

4. Information and communication - these elements focus on the nature and quality of the information needed to implement an effective control. The information must be communicated from top to bottom, organized in a form and in a timely manner that will allow all responsibilities to be fulfilled.

Information plays a critical role in a bank, as it is constantly growing, thus creating conditions for the accumulation of experience, contributing to the development and adoption of effective decisions by management. Banks can have enormous opportunities to accumulate large amounts of information for business, at the same time, the information needs of banks continue to grow steadily, but most often, they fail to have all the necessary information. Therefore, the sooner this problem will be solved, the sooner conditions will be created for the formation of a stable and reliable banking system in the Republic of Moldova.

From the internal control point of view, the information quality plays a key role in the management's ability to make the right decisions, therefore, information must be relevant, reliable, current, timely, complete, accessible, comparable and should be sufficiently prepared for use. However, the information requirements fulfillment can only be achieved by owning developed information systems. Moreover, modern information technologies contribute to the development of information processing technology without using of the paper documents, and the number of types of electronic documents that have the same legal status as paper ones is constantly increasing. Thus, it becomes possible to implement the concept of complete management of electronic documents by facilitating the transfer of data almost instantaneously, the uniqueness of storage, improved security as well as a sharp decrease in the intensity of the workforce of document processing.

Information and communication technologies have a considerable effect on improving the efficiency of the information process and influence both external and internal information systems. External information systems based on information technologies have emerged because of the fast information technology and telecommunications development, subsequently having a huge impact on the development of the entire world banking activity. The most important international information systems known are the International Banking Telecommunications Company (SWIFT), the Reuters system, the Internet. Banks need to make greater use of the information systems capabilities mentioned above in their activities to expand their qualitative boundaries and integrate international financial markets.

The integration of the information system (the ability of all its components to operate on a single database in the bank) is an important aspect in streamlining internal control, so the information of any subsystem is available in real time for all other subsystems. The automation system integrated in the bank needs to have a specific architectural structure, which implies special requirements for applications, technical equipment and communication facilities. Thus, the architecture of information systems and the acquisition of new technologies are important aspects of the bank's strategy, and the selection of the type of technologies used can be essential to objectives' achievement. In order to provide services to customers, the banking activity requires the organization to develop an operational and convenient system of services as in any branch of the bank as well by creating the possibility of remote self-service, thus, such opportinities are accessible only by using ICT solutions and devices (online banking, ATMs, terminals etc.).

In order to combine the information needed for risk management, banks have improved their technology architecture to allow the use of large amounts of data. Web-based information strategies allow real-time data capture, maintenance, and distribution between units and functions, thus,

allowing a better control of multiple data sources. These strategies provided the opportunity to minimize manual processing and automate data analysis and reporting. The use of eXtensible Business Reporting Language (XBRL), eXtensible Markup Language (XML) and web services standards facilitates the aggregation and transfer of data between different intrabank and interbank systems as well as between applications and consequently automates the financial reporting process that leads to its efficiency improvement. Moreover, the XBRL standard allows management and auditors to verify quickly the information at any level of consolidation, either in an operating unit or at the entity level, which also facilitates the rapid identification of the actions required by management. The cost of compliance is also reduced by providing a more efficient platform for communication with regulators, creditors and other parties [2].

As well, banks have highly complex developed information systems that allow real-time monitoring of operations, allowing employees and management immediate access to financial and operational information for more effective control over the bank's business. For the purpose of efficient risk management, entities record and use both historical and current data, but IT systems allow tracking of compliance of effective indicators with expected objectives, plans and expectations. Therefore, these data allow management to assess in real time the existing risks of a particular process, function or unit and to monitor performance; therefore, this information becomes fundamental for effective risk management. Moreover, the growing reliance on information systems at strategic and operational level generates new risks, such as risks of information security breaches or Internet crime, which should be taken into account during the risk management process.

Communication is essential for creating an appropriate internal environment and supporting the other internal control components. In addition to information flows from top to bottom, communication channels should be adjusted to facilitate the communication of information within bank structures or processes. Communication failures can occur when employees are not encouraged to provide important information to other subdivisions or to management or simply do not have the ability to do so. In order to inform management, it is necessary to have open channels for the transmission of information and the availability of management to perceive such information. The channels frequently used for the distribution of information both internally and externally such as the Internet, web pages, e-mails, instant messages, online discussions, web broadcasts, cloud technologies have an enormous impact on the efficiency of continuous communication. The internal communication often used is the intranet site, which can incorporate information on risk management, discussion forum, policies and procedures, contact details of bank employees, etc., with easy and constant access for all staff of the bank. Withal, technology solutions have the possibility of creating separate communication channels as a safety mechanism in case the usual channels do not work.

5. Monitoring - the purpose of this element is to determine whether the internal control is properly designed, correctly executed and evaluates its efficiency. Internal control is properly designed and performed if all five internal control components are present and operate as intended. Many banks that have suffered losses due to internal control problems have not effectively monitored their internal control systems. Often the systems did not have the necessary ongoing monitoring processes in place, and the carried out separate assessments were either inappropriate or not used properly by management [4]. The impact of ICT on continuous monitoring activities, regular monitoring and the internal control evaluation process within banks is reflected in the methodologies and tools used. Methodologies and techniques that could use ICT solutions and equipment to facilitate the evaluation process include the elaboration of the data flow diagram, risk and control matrices,

questionnaires, risk assessment and control workshops, etc. As most financial reports are now generated online and in real time, along with the new electronic technologies that continue to improve, new major challenges have arisen for internal auditors, especially in the area of the efficiency of the internal control system. Thus, auditors need to understand as accounting and internal control as well as information systems to have adequate IT skills to prepare financial statements and assess the correctness of the computer applications processing, which will allow the efficient performance of the audit [5]. Moreover, ICT may be involved in the evaluation of data and transactions based on pre-established criteria and may report the occurrence of inappropriate or unusual elements, which could affect the bank's ability to either implement its strategies or set and realize its objectives. Therefore, the automation and incorporation of the monitoring process into the banking business reflects an important contribution in streamlining internal control.

2. CHALLENGES RELATED TO THE IMPLEMENTATION OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Banks implement the internal control system to minimize potential risks, however, the effectiveness and value of control can be assessed by the costs and the extent to which it reduces the expected risks [6]. In addition to the benefits of information and communication technologies, which relate to reducing the cost of the transaction, improving the efficiency of internal control, the quality of information, the operational process and customer service, there are certain shortcomings that banks have to deal with. Maintenance costs and the need to operate in accordance with certain security measures, including maintaining data security, but also the fact that the person involved in the processing of data by using information technology cannot be tracked in case of errors, represent some of the ICT important deficiencies. Thus, the costs of the financial investments needed to ensure adequate infrastructure should be offset by the benefits provided by information technology products. By using computer systems equipped with adequate security mechanisms, as the unauthorized access to data as well as the recording of unauthorized transactions could be avoided. Although the automated processes facilitate a rapid data processing, there is a risk that in case of deficiencies, the error detection or program modification could take a long time [5].

Other challenges of ICT implementation and consequently, of the internal control system in banks are:

- Information systems and infrastructure of insufficiently secured communication networks;
- Constant and rapid changes in technologies;
- The number of technologies faces an imposing growth;
- Customers' preferences and needs are always changing;
- The number of employees is insufficient or they are not properly qualified;
- Management must provide up-to-date technological support;
- Information technologies should correspond to the specifics of the bank's activity;
- The need to educate customers on new information technologies [3].

The advent of new technologies that are changing the way customers interact with money through the penetration of smart devices and the high speed of the Internet as well as the competition of banking services have had a huge impact on the digital transformation of banks. Therefore, with the creation of opportunities for the digitalization of financial services, banks' exposure to cybercrime (data theft, compromised accounts, destroyed files, etc.) and disruption of information systems could be affected.

In order to minimize these risks, banks must constantly develop and modernize their IT infrastructures with modern risk management technologies such as artificial intelligence, automatic data aggregation, robotic processes optimization, natural language processing, etc. A single approach cannot be established for several banks as each of them has different business strategies and organizational structures, nevertheless, they should follow a balanced strategy of information security risk.

CONCLUSIONS AND RECOMMENDATIONS

Information and communication technology is present in practically every stage of the bank's activity, facilitating efficiency and performance, offering the possibility of instant communication, real-time transaction processing and fostering relationships with customers, investors and other parties. Information technologies are characterized by the use of highly efficient information systems based on the latest technologies, programs and IT solutions for automatic data processing, which promote the reception of information related to regulations, scientific-methodological, planning, accounting, analytical, control and other types of information. As well, the use of advanced technologies allows the prevention of fraud in the field of money laundering, identity fraud or operational errors. At the same time, there are many challenges and risks related to the implementation of ICT, so the monitoring and surveillance of data processed by information systems should be continuous, including manually. Otherwise, banks could generate data and software losses due to deficiencies in hardware, systems and electronic information security as well as data recovery procedures. Proper training of employees in the field of information technology within bank also represents a necessary element for the effective implementation of internal control. As a result of this study, it can be stated that the involvement of information and communication technology can increase the quality and efficiency of the internal banking control system showing an impact on each of its components. Automation of banking processes and the use of advanced information technologies has become essential for banking, which can turn into a less flexible process and even result in its attractiveness. Thus, banks need to identify the real ways to incorporate ICT into the control system, in particular taking into account the risks associated with technologies in the context of the increasing trend towards digitalisation of banking services.

BIBLIOGRAPHY

1. Basle Committee on Banking Supervision. *Framework for Internal Control Systems in Banking Organisations.* Basle, 1998. [pdf] [accesat pe 01.08.2020]. Disponibil: https://www.bis.org/publ/bcbsc131.pdf.
2. Committee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management – Integrated Framework*. 2004 [pdf]. [accesat 28.07.2020]. Disponibil*:* https://economia.uniroma2.it/master-science/ba/corso/asset/YTo0OntzOjI6ImlkIjtzOjM6Ijg5NiI7czozOiJpZGEiO3M6NToiNDMwNDAiO3M6MjoiZW0iO047czoxOiJjIjtzOjU6ImNmY2QyIjt9
3. European Monetary Institute. *Internal control systems of credit institutions*. 1997 [pdf] [accesat pe 29.07.2020] Disponibil: https://www.ecb.europa.eu/ecb/access_to_documents/document/emi_pubaccess/shared/data/ecb.dr.paremi2007_06_report.en.pdf?68a64a898adeb2c786025e142d17db1e
4. GAMAGE, C. T., LOCK, K. L., Fernando, A. A. J. Effectiveness of internal control system in state commercial banks in Sri Lanka. *International Journal of Scientific Research and Innovative Technology*. 2014, vol. 1(5), p. 25–44. [pdf] [accesat pe 01.08.2020]. Disponibil: http://www.ijsrit.com/uploaded_all_files/1633729483_o2.pdf

5. IACHIMOVSCHI, Anatolie. Rolul tehnologiilor informatice în exercitarea misiunilor de audit financiar. *Conferința Științifică Internațională "Competitivitatea și inovarea în economia cunoașterii", (22-23 septembrie 2017). 2018. p. 90-94.* [pdf] [accesat pe 29.07.2020]. Disponibil: https://ibn.idsi.md/sites/default/files/imag_file/90-94_0.pdf
6. PATHAK, Jagdish. *Information Technology Auditing: An Evolving Agenda*. Strauss Offsedruck, 2005, p.154. ISBN 3-540-22155-7.
7. WHITTINGTON O. Ray, DELANEY R. Patrick. *Business Environment and Concepts*. John Wiley &Sons Inc, 2013, p. 64-90. ISBN 978-1-118-27721-8
8. АВДОШИН С.М., ПЕСОЦКАЯ Е.Ю. Информационные технологии для управления финансовыми рисками. *Моделирование и анализ бизнес-процессов.2011, nr. 1(15). [pdf]* [accesat pe 27 august 2020]. Disponibil: http://ecsocman.hse.ru/data/2011/11/28/1270195308/42_2011_1.pdf
9. ЩЕРБАКОВ В. В. Система информационного обеспечения внутреннего контроля в коммерческом банке. Аудит и финансовый анализ [online]. 2000, nr.4, p. 30-77 [accesat pe 10.01.2020]. Disponibil: https://auditfin.com/fin/2000/4/fin_2000_41_rus_02_01.pdf
10. http://www.bnm.md