ARTICLE HISTORY: Received: September 03, 2021 Accepted: October 27, 2021 Published: November 03, 2021

УДК 336.71

ORGANIZING INTERNAL CONTROL OVER ELECTRONIC BANKING SYSTEMS

Yousef Ragheed
Postgraduate student in the Department of Finance, Investment and Innovation Belgorod State University

Abstract. The contribution of technology in the field of banking led to a qualitative shift in the nature of banking and in the mechanism of providing banking services. Electronic banking services have achieved many benefits for both the bank and the customer. In the context of the Russian banking market, the article shows that there is an upward trend in increasing the volume and number of electronic banking transactions executed. The article focuses on the nature of electronic banking services and the new risks that came with them, and highlights the importance of internal control in controlling these risks and reducing them as much as possible. It proposes a development mechanism for internal control, guided by several factors.

Keywords: bank, e-banking, internet, risk, internal control, information security.

Introduction

The main factor affecting literally all spheres of the modern economy is the factor of technological development. Over the past 20 years, there has been a technological revolution unparalleled in history. The advent of electronic means for accumulating and processing information has significantly reduced labor costs, and with the advent of the Internet, an era of unlimited accessibility of information has begun. At the same time, it should be noted that the usual conservatism in the work of banks has remained. It manifests itself in the field of banking security, the principles of lending and fundraising (principles of urgency, payment, repayment)[7].

The successive economic crisis, in addition to objective difficulties, exacerbated competition between commercial banks, and the competitiveness of banks became largely dependent on the convenience of providing services, forcing them to find ways to reduce their costs: reducing the list of additional services, and closing low-profit remote representative offices. At the same time, issues of retaining old customers, attracting new customers, and ensuring stability and high speed of operations remain topical issues [1].

One of the currently popular methods of banking operations is remote, in which the client does not need to visit the bank in person, which can significantly save time. Of the various types of remote banking services, electronic banking systems stand out.

The advantages of electronic banking lie in the technology itself. Provides the possibility of round-the-clock remote access to account data, management of banking operations continuously and from any place where there is the possibility of using the Internet or cellular communication. Note that with the help of remote banking services, not only the list of potential client opportunities is expanded, but also the bank's funds are saved, which are spent on maintaining additional offices and representative offices in remote areas.

Currently, we can actually talk about electronic banking systems that focus on legal entities (corporate systems) and individuals (population systems). Moreover, the peculiarity of the Russian market for electronic banking services is that corporate systems currently dominate in terms of the volume of electronic transactions, but at the same time they actually have much less potential to expand the customer base compared to the systems for individuals. This is due to the fact that remote work systems with legal entities were installed long ago in almost all domestic banks. According to BSS, Bank-Client systems are the most in-demand among banks. Corporate systems development is linked to the development of specialized solutions to serve legal entities, in which the 'bank-customer' system is an integral part [9].

There is a large number of banks that provide electronic banking services to individuals in Russia, and there is a trend of continuous increase in the number of systems used for individuals. According to market experts, the potential for developing online banking services is enormous. The number of users of electronic banking services in Russia is expected to reach 40 million during the next few years[2].

An additional factor in the development of electronic banking systems for the population is the parallel development of mobile communications. The number of mobile subscribers now significantly exceeds the population of Russia. It can be argued with a high degree of probability that mobile services will show a steady increase in the customer base in the coming years. Thus, the Russian Internet banking market is gradually increasing the pace of its development, including using the possibilities of integration and development of other complementary services.

The main part

Credit institutions provide a variety of sets of electronic banking services. Today, Russian consumers have the opportunity to compare, choose and use electronic banking services. In general terms, we can talk about the following main operations that can be carried out through electronic banking systems:

- implementation of all utility payments (electricity, gas, heat supply, etc.);
- payment of bills for communications (telephone, cellular, Internet, cable and satellite TV);
- money transfers to any account in any bank;
- transfer of funds to pay bills for goods, including those purchased through online stores;
- buying and selling foreign currency;
- replenishment / withdrawal of funds from the plastic card account;
- preliminary registration of various types of accounts (urgent, savings, pension) and transfer of funds to them;
- obtaining an account statement for a certain period in various formats;
- receiving information about funds received to a bank account in real time;
- receiving information about the payments made;
- receiving other services: subscription to magazines and newspapers, brokerage services (purchase / sale of securities, creation of an investment portfolio, the ability to participate in the bank's mutual funds, participation in trading, etc.) [10].

If you pay attention only to the advantages and capabilities of the electronic banking system, then it may be believed that the introduction of such technology of remote banking does not pose any threats and only leads to a decrease in costs, an expansion of the circle of potential customers, an increase in the speed of transactions, etc.

In fact, this is the visible part of the iceberg. All the "most interesting" is inside the bank itself - in its organization, processes, which, as a rule, are not ready to perceive the new reality. New sources of threats cannot create a rosy picture for the bank, but lead to serious problems associated with a decrease in the level of reliability of the banking automated system and threats to information security [8].

Due to the rapid technological development of modern society and the fiercest competition in the banking business, most bank managers (as well as other companies) succumb to the temptation to use technological innovations as soon as possible. Such hasty innovations lead to a decrease in the quality of management decisions in terms of an adequate strategic assessment of the development of the organization. The consequence of this is subsequent technical failures, inconsistencies in business processes, a decrease in the overall level of bank security, which ultimately leads to significant financial losses.

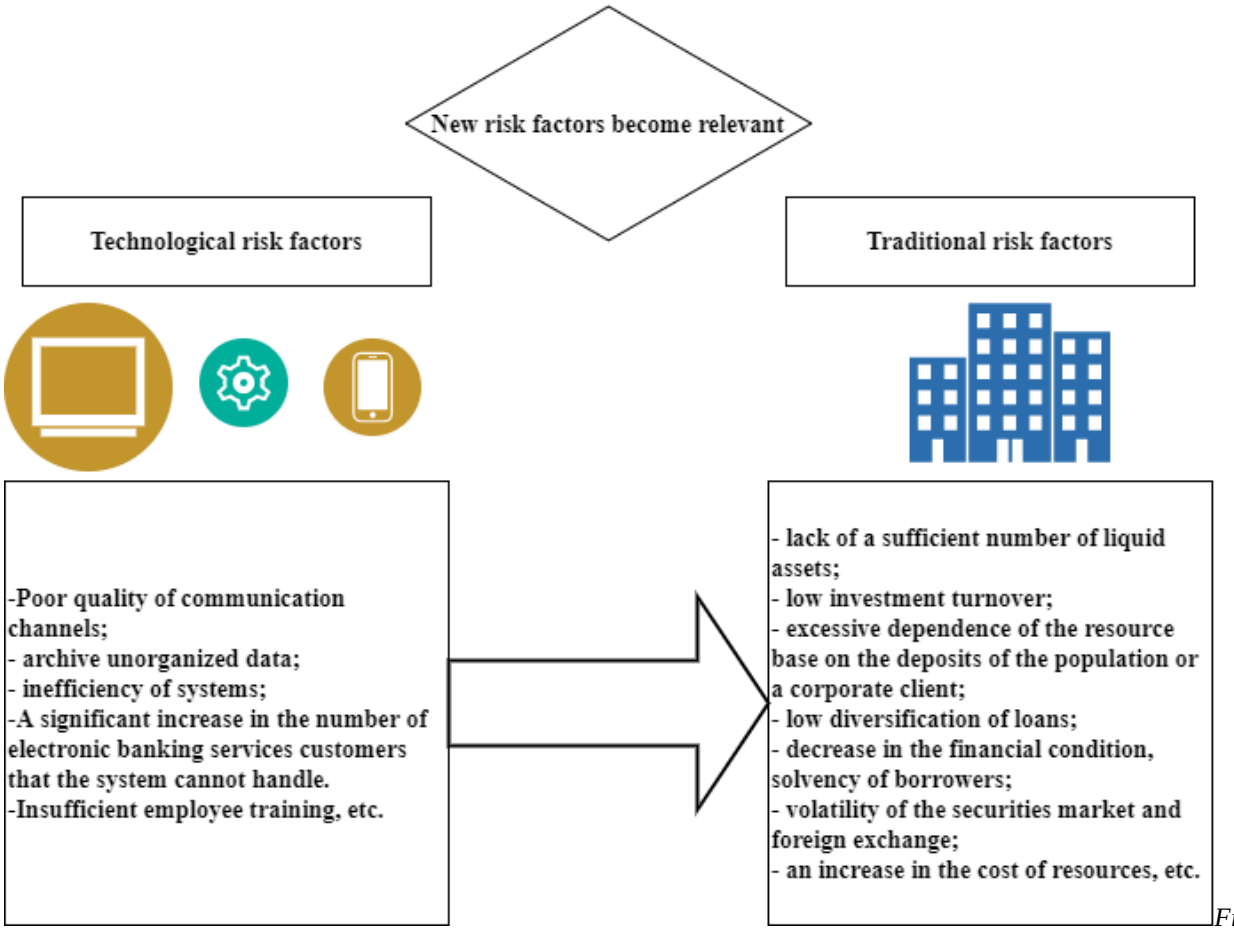
One of the reasons for the complexity of adapting the electronic banking system to an already operating traditional banking system is the lack of a strategic vision for developing the current system. In a number of cases, software developers are making changes to the automated banking system, in part. As a result, so-called "bottlenecks" appear, which are, in essence, sources of various banking risks.

The emergence of such "bottlenecks" leads to a violation of the security of the electronic banking system, as access is opened from outside to previously closed data, or integrated systems are adversely affected by each other.

It is clear that the use of electronic banking technology greatly increases the credit institution's reliance on information technology and, as a result, increases the technical complexity of many functional and security tasks. Another distinguishing feature of the present day is the increasing dependence of credit institutions on different types of service providers, many of which are not subject to any kind of regulation. This development has led to the emergence of new business models that include banks and non-banks such as Internet service providers, telecom companies, and other technology companies [3].

The expansion of business models through the participation of different types of "third parties" has led to the emergence of new sources of banking risks associated with technological factors (Figure 1).

In this case, the list of risks remains the same, and the role of the technical component of its list increases. It is important for senior bank managers to understand this. Usual control methods and risk management processes must be adapted to the technological components.



Figs. 1. The trend of changes in banking risk factors

Otherwise, the bank's electronic systems become vulnerable to:

– technological distortion of processed banking information, which exacerbates the issue of the reliability of bank statements generated in the information circuit, and causes difficulties in exercising control over the execution of banking operations in electronic form;

– deliberate violation of information flows and communications, theft of confidential banking information, implementation of other illegal actions;

– the emergence of dependence on communication service providers, since some of the equipment and databases of the information circuit, one way or another, are controlled by them and are not subject to any monitoring by the credit institution.

It is obvious that the new reality and the issues of uninterrupted functioning that credit institutions and their clients are forced to face when using electronic banking technologies require modernization, and in some cases a serious revision of the procedures for monitoring and countering risks [4].

Considering the organization of the use of electronic banking systems, it is necessary to single out the processes of the "upper level", which determine the strategic focus of the credit institution on the development of technologies of electronic banking and the processes of the "lower level", which directly determine the processes of safe use of electronic banking systems.

As for the processes of the "lower level", which actually make up the architecture of the secure use of electronic banking systems, you should immediately pay attention to the fact that, due to individual approaches to the structure of intrabank distributed computer systems (which means an individual set of requirements for ensuring the integrity and security information resources, an original set of methods and means of risk control), it is difficult to propose processes for the safe application of electronic banking systems that are universal for all banks. The internal control system of a credit institution should play a special role in organizing control over risks (including in connection with the introduction of various systems of remote banking services).

In accordance with the Regulation of the Bank of Russia dated December 16, 2003 No. 242-P "On the organization of internal control in credit institutions and banking groups," the concept of "internal control system" is defined as a set of internal control bodies and areas that ensure compliance with the procedure for implementing and achieving goals

established by the legislation of the Russian Federation, regulatory legal acts of the Bank of Russia, constituent and internal documents of the bank [6].

Control is an integral part of any management system and a condition for a credit institution to achieve its goals. In addition to control functions, the internal control system ensures the solution of the following tasks:

- minimization of costs (including payment for the services of an external auditor);
- providing the management of the credit institution with the necessary information on deviations from the established regulations;
- tracking risks and taking a set of measures to help reduce them;
- resolving conflicts of interest arising in the course of a credit institution's activities.

When developing and implementing an internal control system, it is advisable to be guided by the following principles [5].

1. Principles related to the internal control system as a whole and contributing to the efficiency of banks. The internal control system should be:

- comprehensive, covering all possible types of activities, special attention should be paid to financial innovations;
- adapted to prevent and detect fraud and other violations;
- linked to the information and communication system operating in the credit institution in order to ensure the flow of information necessary for control;
- suitable for the relevant regulatory framework.

2. Principles relevant to the organization of the management system. Each credit institution should have a management system adapted both to the nature, scale and complexity of the activities it performs, and to the risk factors inherent in these activities. The banking model depends on the industry focus of the bank, the market segment in which it operates, the size and range of banking products offered to its customers. Establishing and maintaining an appropriate management system is one of the most important aspects of an internal control system.

At the same time, the organizational structure should be clearly defined, within which responsibilities are allocated and the reporting procedure established.

An efficient division of responsibilities eliminates the possibility of manipulation and error. It is important that internal control mechanisms operate independently of the units whose activities are subject to control:

- employees must be able to carry out their duties. At the same time, only authorized employees of the credit institution are provided with access to assets and information;
- procedures for conducting all operations should be documented and personnel familiar with these procedures;
- Appropriate control procedures should be established for each process so that all transactions are authorized, recorded and processed in the prescribed manner.

3. Principles related to risk management. Systems for managing risk factors that can be quantified should be developed, namely, a process for identifying risk factors and monitoring the degree of risk to which the bank is exposed should be established. For non-quantifiable risk factors, every effort should be made to minimize the risk.

4. Principles related to information systems. To ensure that an effective information system is in place, the following conditions should be considered:

- accurate information about each recognized valid transaction must be recorded for the period during which the transaction was performed, in a timely manner and with sufficient detail;
- an “audit trail” is required so that all transactions can be traced in chronological order. The “audit trail” should include information on transactions recognized as invalid (information should be based on original documents to explain changes in the bank balance of funds recorded on a particular date, compared to the date of the previous report);
- the board of directors, management and other employees must be able to receive timely information sufficient to fulfill their official duties;
- information for external users (annual reports, etc.) must meet the established requirements.

5. Principles related to electronic information systems. The use of information technology is associated with additional risk factors. Loss of data and programs, failure of equipment or systems, inaccuracy of information used in the management process, and other factors can turn into serious problems and jeopardize the ability to continue operations or lead to a situation where decisions can be made on the basis of inaccurate or intrusive misleading information.

A fairly good approach to solving issues of control over the functioning of systems was proposed in the Bank of Russia information security standard STO BR IBBS-1.0-2010 [3], where it is recommended to organize management on the basis of a model of a continuous cyclic management process (Deming's model). It identifies four main stages in the operation of any system: planning, implementation, verification, improvement.

Based on this model, the authors of the article propose a detailed model of the life cycle of an electronic banking system (see Fig. 2).

When describing the procedures for the safe use of electronic banking systems, we will mean the following:

1. Refinement and modification of the electronic banking system should be carried out on the basis of a "life cycle", where the implementation of appropriate actions and procedures at each stage is assumed.

2. The specificity of adaptation of the main intrabank business processes to the operating conditions of electronic banking systems should ensure the continuity of the risk control process in all areas of the system operation and in all structural divisions of the credit institution involved in the work, and should also cover its interaction:

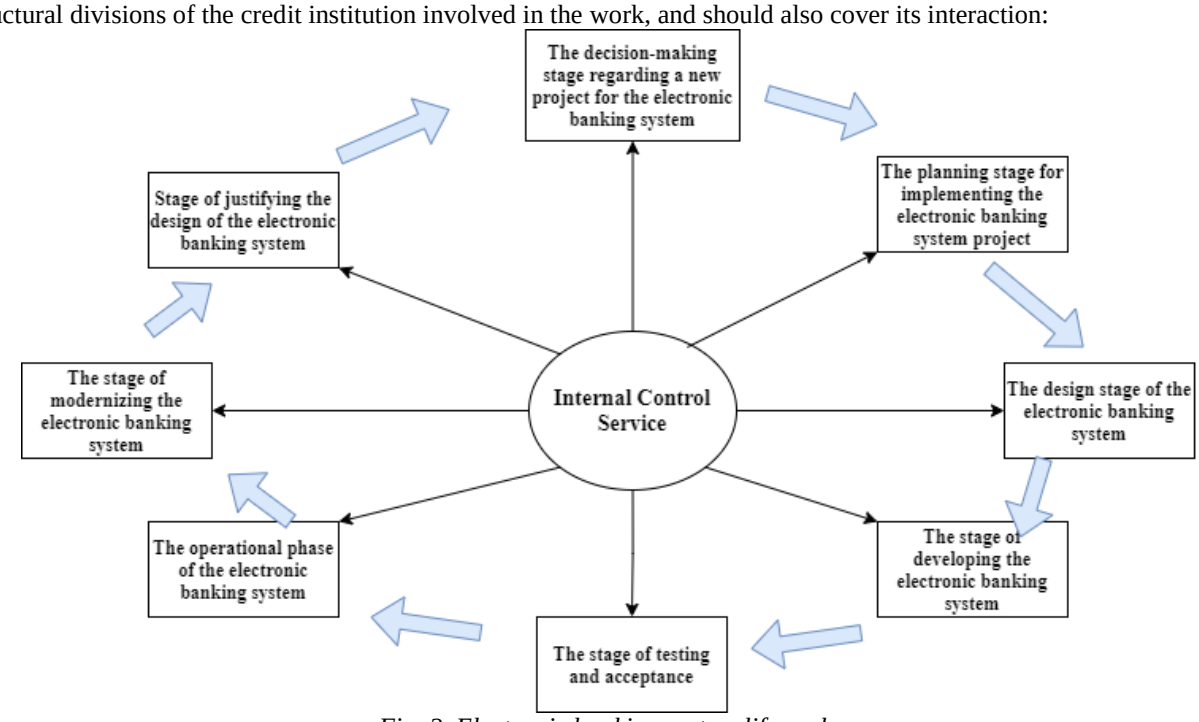


Fig. 2. Electronic banking system life cycle

– with clients (both legal entities and individuals) using electronic banking systems;

– with counterparties, which may include providers, hardware and software suppliers, as well as other third-party organizations, for example, providing consulting, repair and adjustment services, promoting the services of a credit institution in the form of electronic banking in the banking market among legal entities and the public through specialized marketing PR-actions and programs.

3. The safe organization of the electronic banking system can be obtained with the proper orientation of the "upper level" processes towards the future development of such systems.

Indeed, an organization without strategic goals or corporate values is extremely difficult to operate. It is good practice when the general strategy of the bank reflects issues related to the development of not only information technology, but also remote banking systems.

At the same time, the board of directors should devote sufficient time to discussing the development strategy, including identifying priority areas for development in the field of remote banking technologies (in particular, electronic banking technologies). That is, the strategic plan of a credit institution should reflect plans for the introduction, application and development of electronic banking technologies, quantitative and qualitative indicators that allow assessing the bank's activities in the electronic area of the market.

In order to effectively manage the risks arising when a credit institution conducts operations using electronic banking systems, it is necessary to ensure that the plans for the implementation and development of electronic banking services are in line with the strategic goals, and the possible consequences of the decisions taken must be weighed against the maximum permissible aggregate level of risk that the credit institution can accept, having stipulated in internal documents. Otherwise, the adoption by the governing bodies of the credit institution of erroneous decisions regarding the implementation, maintenance and development of electronic banking systems may lead to losses, the reasons for which may be:

– high costs for the implementation and maintenance of the electronic banking system;

– the impossibility of achieving the set strategic goals due to the lack or not being provided in full with the necessary resources (financial, technical, material and human);

– failure to comply with organizational measures in the field of electronic banking technologies;

– errors in the implementation of organizational and technical solutions when introducing an electronic banking system.

A high-quality development strategy should provide for procedures for a timely and adequate response to possible actions of the credit institution's competitors or the emergence of new technological solutions. The absence of such a provision can lead to a loss of competitive advantage in this area and lead to an outflow of customers using electronic banking technologies.

Conclusion

The introduction of electronic banking technologies also significantly increases the qualification requirements for the top management of a credit institution. After all, it is important not only a high-quality organization and conscientious execution of all procedures for the safe use of such systems, but also the quality of the perspective thinking of top managers in terms of maintaining and developing the bank's technological advantages. In this regard, it seems appropriate to have a manager in the senior management of a credit institution who has sufficient training in the field of distributed computer systems in general and an understanding of the construction of informational contours of banking and the risks associated with this area. Therefore, such an employee from the top management, whose responsibilities include the organization of information technology management, are recommended to undergo periodic training (retraining) on electronic technologies and the specifics of their application. Similar recommendations apply to the board of directors.

If the board of directors includes specialists with education in information technology, it will be able to properly monitor the compliance of the organization and functioning of electronic banking systems with the content of the main activities of the credit institution, as well as make informed strategic decisions regarding:

- introduction of new technologies of electronic banking;
- maintaining an appropriate marketing policy;
- definition of tariff plans;
- the content of contracts with customers, contractors and providers.

Not only the quality of business processes at all stages of the use of electronic banking systems, but the reliable and uninterrupted operation of the entire bank as a whole directly depends on the degree of involvement of the senior management and owners of the bank in the development of electronic banking technologies.

In conclusion, I would like to note that such an approach, in our opinion, can be taken as a basis for adapting internal control procedures in a credit institution, since it is aimed at minimizing risks through the end-to-end application of control procedures and assumes the possibility of taking into account the specifics of specific credit institutions, including their information circuit.

References

1. Akter S., Motamarri S., Hani U., Shams R., Fernando M., Babu M. M., Shen K. N. Building dynamic service analytics capabilities for the digital marketplace // Journal of Business Research. -- 2020. -- Vol. 118. -- Pp. 177-188.
2. Belousova V., Chichkanov N. Mobile Banking in Russia: User Intention towards Adoption // Foresight. -- 2015. -- T. 9, № 3 (eng). -- C. 26-39.
3. Berdyugin A. A., Revenkov P. V. Approaches to measuring the risk of cyberattacks in remote banking services of Russia // Bezopasnost' informatsionnykh tekhnologiy. -- 2019. -- Vol. 26, № 4. -- Pp. 83-92.
4. Fliginskih T., Vaganova O., Solovjeva N., Bykanova N., Ragheed Y., Usatova L. The impact of e-banking on performance of banks: Evidence from Russia // Journal of Advanced Research in Dynamical and Control Systems. -- 2020. -- Vol. 12, № S4. -- pp. 231-239.
5. Risk management in electronic banking: Concepts and best practices. / Kondabagil J.: John Wiley & Sons, 2007. -- 365 p.
6. Korobeynikova O. M., Korobeynikov D. A., Popova L. V., Savina O. V., Kamilova R. S. The current state of the payment infrastructure and development of payment systems in Russia and the Volgograd region // Revista Espacios. -- 2017. -- Vol. 38, № 62.
7. Taylor S., Todd P. Assessing IT usage: The role of prior experience // MIS quarterly. -- 1995. -- C. 561-570.
8. Vaganova O., Bykanova N., Grigoryan A., Cherepovskaya N. Directions of development of bank technologies applied in the Russian market of retail credit services // National Academy of Managerial Staff of Culture and Arts Herald. -- 2018. № 3. -- Pp. 382-387.
9. Vdovina A., Bass A. Payment tools in the mobile banking // Ekonomika i biznes: teoriya i praktika. -- 2020. № 4-1. -- Pp. 55-66.
10. Abu-Alrop J., Kokh I. Impact of Credit Risk on the Performance of Russian Commercial Banks // Journal of Applied Economic Research. -- 2020. -- Vol. 19, № 1. -- Pp. 5-18.