Complaens Risks of Using It Technologies in Banks in the Period of Digitization

Sherzod Fayziev
Researcher at Tashkent State University of Economics,
Tashkent, Uzbekistan

Abstract. **The use of end-to-end technologies in the activities of banks makes it possible to speed up many banking processes, increase the loyalty of existing clients and attract new ones, and, as a result, increase the profitability and competitive position of banks. Today banks use a distributed registry system, Big Date, virtual and augmented reality, artificial intelligence, and robotics. However, their implementation is associated with a number of problems and risks both on the part of the banks themselves and their clients. The article highlights the most significant problems and risks of using end-to-end technologies in banking: cyber risks, fraud, the creation of ineffective parallel data warehouses, decentralization due to the complication of IT systems, compliance risks, excessive interdependence of participants leading to operational and systemic risks.**

Keywords: End-to-end technologies, cyber risks, artificial intelligence, robotization, banks.

1. INTRODUCTION

The republic is implementing comprehensive measures for the active development of the digital economy, as well as the widespread introduction of modern information and communication technologies in all sectors and areas, primarily in public administration, education, healthcare and agriculture.

In particular, the implementation of over 220 priority projects has begun, providing for the improvement of the e-government system, the further development of the domestic market for software products and information technologies, the organization of IT parks in all regions of the republic, and the provision of qualified personnel in this area.

In the context of strengthening the position of the digital economy in Uzbekistan, new requirements will undoubtedly be imposed on internal control, compliance control and internal audit. And this will primarily be associated with the expansion of the information base of all types of control and audit. The latter will allow the use of a larger scale of control methods, audit evidence and will strengthen the role of economic analysis, which allows us to identify risk areas in the activities of the audited entity and justify the feasibility (reality) of the proposed strategy and investment plans.

2. LITERATURE REVIEW

The study is based on scientific works in the field of research by I. A. Ezangina, A. V. Evstratov [1], E. B. Starodubtseva, M. B. Medvedeva [7], E. V. Popov [6], O. L. Koroleva [2], E. V. Usenya [9]), the structure of entrepreneurial ecosystems and interactions of participants (E. Lafuente et al. [14], M. Palm [15], E. Gianluca [12], A. Kapturkevich [13], Tretyakova E. A., Freiman E. N. [8]). The scientific literature has developed approaches regarding the types of crowdfunding and their financial conditions.

3. ANALYSIS AND RESULTS

Possible risks for investors and borrowers are associated with the likelihood of loss of investor income in the event of ineffectiveness of the project, a decrease in the time value of money under the influence of inflation, low liquidity of shares, economic instability, and insolvency of the borrower or unattractiveness of the entrepreneurial idea [1; 3; 10]. Compliance risks caused by non-compliance with the requirements and rules of the platform have a deterrent effect - losses due to fraud and deception, the organization of financial pyramids and unlicensed transactions, failure to fulfill contractual obligations, lack of control over the intended use of funds, loss of rights to a digital asset, violation of the rights of shareholders, unreliability of platform participants and changes in legislation [1; 2; 4; 9]. Kuvaeva Yu. V. and co-authors [3], G. T. Papascua [5] draw attention to the high risks of unreliable information posted on the digital investment platform and the low level of awareness of transaction participants.

In a risk situation, it is necessary to identify risk factors and develop measures to reduce them. To this end, it seems necessary to consider the digital investment platform as an ecosystem and highlight the key participants, their role and network relationships.

If you look in the Oxford English Dictionary, the term compliance (from the English compliance - agreement, compliance; comes from the verb to comply - to comply) is presented as an action in accordance with a request or instruction. In banking, the concept of "compliance control" is very common, where compliance is an integral part of the internal control function, "the purpose of which is to protect the interests of investors, banks and their clients by monitoring compliance by bank employees with the provisions of current legislation, requirements of supervisory authorities, as well as documents defining the internal policies and procedures of the bank. Compliance control is considered as the principle of conducting business by a financial institution in accordance with applicable laws, regulations, codes and standards established by competent authorities, professional associations and internal documents of the financial institution. This definition indicates the special importance of compliance control as a principle of business conduct, and also specifies those documents, the adherence to which a financial organization considers an important area of activity [2].

Compliance (eng. Compliance - agreement, conformity; comes from the verb tocomply - to perform) - literally means action in accordance with a request or instruction; obedience. Analyzing the collection of definitions, we can formulate the integrated concept of "compliance control" - this is a risk management process aimed at voluntary compliance with government legislation, as well as ethical standards adopted in the field of regulated legal relations and business customs, in order to maintain appropriate rules and standards of behavior in the market , as well as strengthening the image of the company and organization. "Compliance control" is a very broad area and it is characterized by a number of specific areas, such as: anti-money laundering, proceeds from crime, terrorist financing; development of documents and procedures that ensure compliance with current legislation; protection in the field of information flows, anti-fraud, anti-corruption, establishing ethical standards of behavior for bank employees, etc.

Customer expectations regarding support from banks have not changed in terms of what they expected to receive. Artificial intelligence has clearly impacted this situation, with AI-enabled chatbots and voice assistants now becoming the norm at large financial institutions. Banks have a lot of data about their customers. But the data is disintegrated in such a way that while resolving a request, customer service agents need to go through multiple files and folders just to understand what the request is about. When using chatbots in banking, data can be collected, stored and managed in a form that makes it easier to resolve queries. With the speed of conflict resolution by a chatbot, the number of refusals will automatically decrease and the quality of customer service will improve.

It is now possible to implement a new tool called ChatGPT, which went viral in late 2022 by generating answers to human-like questions. However, it is not yet perfect and can generate answers that seem convincing at first glance, but in fact are not always correct. Voice assistants are available in every bank today. For example, a voice robot in a bank's call center allows you to get a consultation 40 seconds faster. As for the chatbot, it processes over 40% of client requests and saves the bank a decent amount.

However, in addition to numerous positive aspects, end-to-end technologies pose a number of problems and risks for the banking industry. Like all technologies whose operation involves the use of the Internet, there is an acute problem of security. And we are talking about both the banks themselves and their clients.

In 2020, the Central Bank established cooperation with Kaspersky Lab to prevent cybercrime and combat theft of funds. The first event within the framework of cooperation was a training for leaders of the country's financial sector and a simulation game on countering cyber-attacks.

Kaspersky Lab is an international company specializing in the development of protection systems against computer viruses, spam, hacker attacks and other cyber threats. The company not only creates protection systems, but also conducts research into the risks that their users are exposed to in different countries. Thus, at the beginning of 2020, the company analyzed data, including for Uzbekistan, noting that the greatest danger to users in the country is posed by ransomware and attacks by miners.[16]

According to the Cybersecurity Center of the Republic of Uzbekistan, in 2021 there were 1.3 million cyber-attacks on sites in the "uz" segment.

Of the 100 thousand domains registered in the national "uz" segment, about 38 thousand are active. Of these, only about 14 thousand domains have an SSL security certificate.

In 2021, the Center detected more than 17 million cases of malicious and suspicious online activity in Uzbekistan. The majority of "pests" (76%) are bots.

Most cyber-attacks were carried out from Uzbekistan, Russia, Germany, the UK and the USA.

Monitoring of information systems and websites of government agencies revealed 636 problems, including technical problems, which amounts to about 1 million 48 thousand minutes of unavailability (downtime) of websites.

Regarding websites of the "uz" domain zone, 444 incidents were recorded, of which the largest number were

unauthorized downloads of content - 341.89 were associated with unauthorized changes to the main page (Deface).

At the same time, public sector websites (134 incidents) are subject to attacks 3 times less often than the private sector (310 incidents).

The main reasons and methods of successful hacker attacks are: an outdated or vulnerable version of the content management system (72%), guessing passwords for accounts (Brute force), SQL injections and outdated plugins.

To improve the level of cybersecurity, the Center recommends:

use licensed and certified operating systems and applications;
regularly update existing operating systems, software and security components;
use security plugins that have search, removal and anti-malware functions;
create backup copies of databases, files, mail, etc.

Cybercriminals are constantly launching attacks. In particular, in 2021, the Tashkent metro was subject to a cyber-attack, and the ticker was hacked at the Gulistan bank. Hackers also attacked the Surkhandarya khokimiyat.

In 2019, the first roadmaps appeared, the essence of which contained such end-to-end technologies as: artificial intelligence, virtual and augmented reality, robotics, sensors, etc. Almost each of them found its application in the banking sector, at the same time giving rise to a number of risks.

Another problem is the creation of inefficient parallel data warehouses. Due to existing information technology and data privacy regulations, such as the protection of personal data, there are difficulties in exchanging information between banks.

In addition, IT requirements lead to more complex technological systems. On the one hand, the Basel standard regulates that IT systems must function centrally. On the other hand, the strategies of specific commercial banks dictate the need for various blocks to work separately, which certainly leads to decentralization.[17]

Some regulators still use outdated reporting portals, reducing efficiency and increasing the likelihood of reporting errors. Updating online reporting portals and secure data transfer mechanisms will significantly improve the efficiency of the process for both regulators and banking institutions. Automated, secure online data transfer mechanisms without file size restrictions can significantly improve reporting efficiency for both regulators and financial institutions.

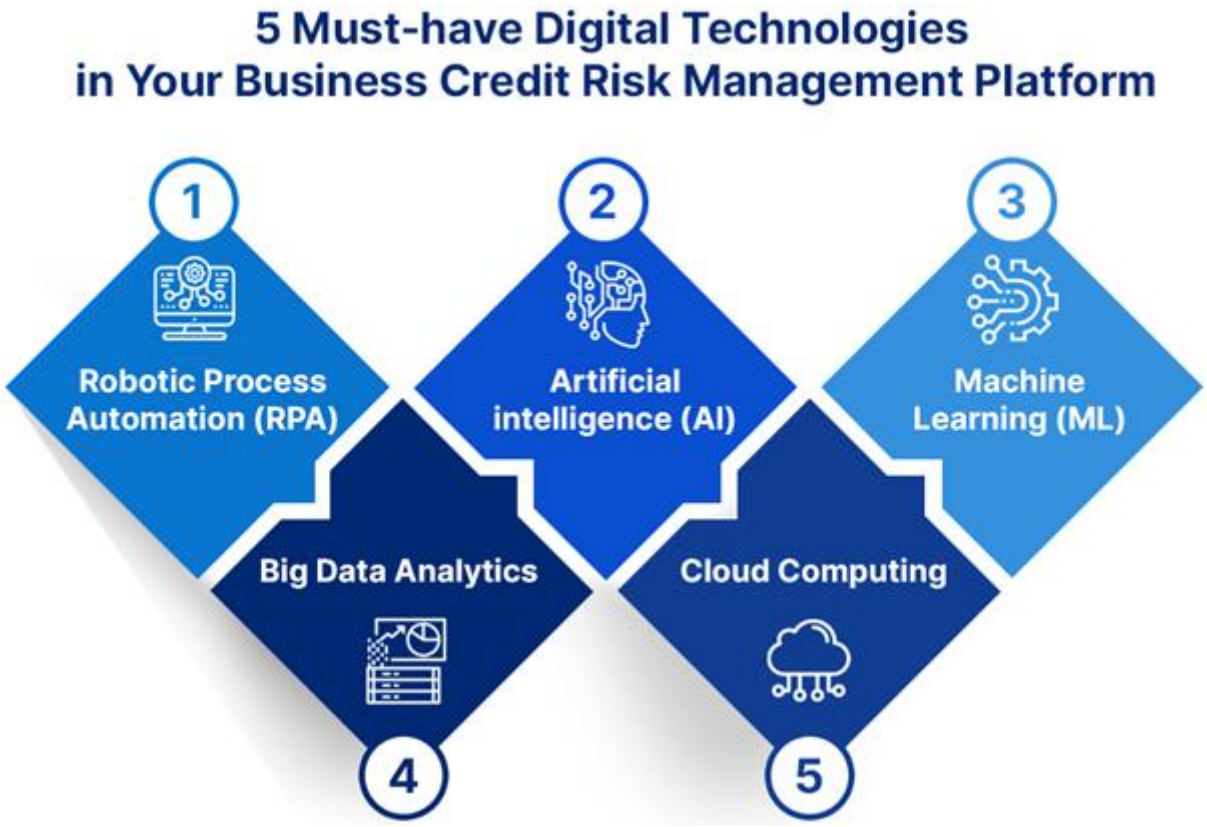

Fig.1. Complains risks of using it- technologies [17]

Anti-money laundering and counter-terrorist financing (AML/CFT) supervision, despite a common international framework, currently differs significantly from one jurisdiction to another. Harmonization of standards by regulators could remove existing barriers to the sharing of suspicious customer and other information within a banking group.

Since all participants in the banking sector basically use the same platforms, if the IT system fails, the situation will develop into a systemic crisis. In other words, the use of end-to-end technologies in the banking sector leads to excessive interdependence of participants. Consequently, if one of the participants experiences technological problems, then the entire banking system, according to the domino principle, may collapse. Do not forget that the complication of the system also leads to an increase in the number of participants. The more complex the system, the more difficult it is to manage, and, consequently, the operational and systemic risks are much higher. The team of experts of the European Systemic Risk Council noted that banks mainly use outdated IT systems, therefore, without the involvement of third parties. For example, the use of cloud technologies, etc.

In addition, low barriers to entry into the market when using end-to-end technologies. In fact, existing participants in the banking market may lose a significant part of their profits if new participants, through the use of the latest developments in the field of technology and technology, are able to offer similar products and services, but, for example, on more attractive terms or at a lower price. For example, attract deposits at higher rates by reducing transaction costs. It is worth noting that in today's environment, deteriorating profitability due to a lack of flexibility in interaction with customers can weaken the ability of existing banking institutions to withstand business cycles.

The use of end-to-end technologies is associated with compliance risks, which include non-compliance with the requirements of the legislation on the protection of personal data in connection with the involvement of third-party organizations. Naturally, such organizations, having gained access to customer data, will try to use it for their own purposes.

Another problem is the reduction of jobs as many processes become more automated. However, it cannot be said that banking activities can be completely automated. Some operations will always require human presence.

4. CONCLUSIONS

To summarize, it is worth noting that the implementation of the Digitalization Strategy in the country until 2030 is gradually gaining momentum, including in the banking sector. More and more end-to-end technologies are being introduced into the activities of commercial banks. Technologies such as Big Data, distributed registries, virtual or augmented reality, artificial intelligence, robotics, etc. are actively used. The obvious advantages of these technologies in the activities of banks are: reducing transaction costs, attracting new clients, developing a new product line, increasing customer loyalty, obtaining competitive advantages and, as a result, increased profits. However, this process also has a downside associated with problems and risks, which we include:

- a security problem that is closely associated with the risk of fraud, cyber risks and the risks of cyber attacks;
- ineffective parallel storage of data instead of a full exchange of information and the absence of duplicate information among different economic agents;
- increasing complexity of IT systems leading to decentralization;
- increasing difficulties in meeting compliance requirements and AML/CFT standards;
- use of outdated portals for reporting;
- excessive interdependence of participants, leading to operational and systemic risks;
- low barriers to entry, which can lead to a weakening of the ability of existing banking institutions to withstand business cycles;
- compliance risks;
- reduction of jobs in banks.

Thus, end-to-end technologies are certainly the future of the banking sector, allowing for significant results in increasing profitability. However, it is worth developing a system of measures, including the use of end-to-end technologies, which will minimize the risks associated with their use.

REFERENCES

[1]. Ezangina, I. A., Evstratov, A. V. (2019) [New tools for financing small and medium-sized businesses in Russia: crowdinvesting]. Finansy: teorija i praktika [Finance: theory and practice]. Vol. 23. No. 3, pp. 122-136.

[2]. Korolev, O. L. (2022) [Financial risks of a virtualized economy]. Nauchnyj vestnik: finansy, banki, investicii [Scientific Bulletin: finance, banks, investments]. Vol. 3. No. 60, pp. 37-45.

[3]. Kuvaeva, Ju. V, Chudinovskih, M. V., Sedunova, E. A. (2021) [Model types of crowdfunding: a comparative analysis of Russian and European experience]. Vestnik NGUJeU [Bulletin of NSUE]. Vol. 4, pp. 121-134.
[4]. Mihajljuk, M. N., Chinazirova, S. K., Kostenko, R. V. (2020) [Crowdfunding as a tool to attract investment in the innovative sector of the economy]. Novye tehnologii [New technologies]. Vol. 16. No. 6, pp. 116-122.
[5]. Papaskua, G. T. (2021) [Crowdfunding: concept, types and risks]. Aktual'nye problemy rossijskogo prava [Actual problems of Russian law]. Vol. 16. No. 7, pp. 77-85.
[6]. Popov, E. V., Veretennikova, A. Ju., Fedoreev, S. A. (2021) [Opportunities and limitations of the development of crowdlending platforms]. Finansy i kredit [Finance and credit]. Vol. 27. No. 11, pp. 2479-2502.
[7]. Starodubceva, E. B., Medvedeva, M. B. (2021) [Crowdfunding as a modern form of financing]. Finansy i kredit [Finance and credit]. Vol. 27. No. 1, pp. 22-40.
[8]. Tret'jakova, E. A., Frejman, E. N. (2022) [Ecosystem approach in modern economic research]. Voprosy upravlenija [Management Issues]. Vol. 1, pp. 6-20.
[9]. Usenja, E. V. (2020) [Crowdfunding: risks for investors]. Vestnik Polockogo gosudarstvennogo universiteta. Serija D. Jekonomicheskie i juridicheskie nauki [Bulletin of Polotsk State University. Series D. Economic and legal sciences]. Vol. 13, pp. 143-147.
[10]. Jacenko, T. S. (2019) [The problem of protecting the rights of investors in crowdfunding: investment risks and ways to overcome them]. Zhurnal rossijskogo prava [Journal of Russian Law]. Vol. 8, pp. 62-71.
[11]. Yakimova, V. A., Pankova, S. V. (2022) [Formation of a methodological model of investment audit]. Uchet. Analiz. Audit [Accounting. Analysis. Audit]. Vol. 29. No. 3, pp. 14-26.
[12]. Gianluca, E., Margherita, A., Passiante, G. (2020) Digital entrepreneurship ecosystem: How digital technologies and collective intelligence are reshaping the entrepreneurial process. Technological Forecasting and Social Change. No 150(1). P. 119791, https://doi.org/10.1016/j.techfore.2019.119791.
[13]. Kapturkiewicz, A. (2021) Varieties of Entrepreneurial Ecosystems: A comparative study of Tokyo and Bangalore. Research Policy. Vol. 51 (9), https://doi.org/10.1016Zj.respol.2021.104377.
[14]. Lafuente, E., Acs, Z. J., Szerb, L. (2021) A composite indicator analysis for optimizing entrepreneurial ecosystems. Research Policy. Vol. 51 (9), https://doi.org/10.1016/j.respol.2021.104379 (In Eng.).
[15]. Palmie, M. et al. (2022) The evolution of the digital service ecosystem and digital business model innovation in retail: The emergence of meta-ecosystems and the value of physical interactions. Technological Forecasting and Social Change, Vol. 177, https://doi.org/10.1016/j.techfore.2022.121496.
[16]. 16.https://www.gazeta.uz/ru/2021/06/30/Kaspersky.
[17]. https://www.emagia.com/blog/5-must-have-digital-technologies-in-your-business-credit-risk-management-platform.