









“Operational risk management of using electronic and mobile money”

AUTHORS	Volodymyr Mishchenko   Svitlana Naumenkova   Andrii Grytsenko  Svitlana Mishchenko  
ARTICLE INFO	Volodymyr Mishchenko, Svitlana Naumenkova, Andrii Grytsenko and Svitlana Mishchenko (2022). Operational risk management of using electronic and mobile money. <i>Banks and Bank Systems</i> , 17(3), 142-157. doi: 10.21511/bbs.17(3).2022.12
DOI	http://dx.doi.org/10.21511/bbs.17(3).2022.12
RELEASED ON	Monday, 19 September 2022
RECEIVED ON	Wednesday, 20 July 2022
ACCEPTED ON	Wednesday, 14 September 2022
LICENSE	 This work is licensed under a Creative Commons Attribution 4.0 International License
JOURNAL	"Banks and Bank Systems"
ISSN PRINT	1816-7403
ISSN ONLINE	1991-7074
PUBLISHER	LLC “Consulting Publishing Company “Business Perspectives”
FOUNDER	LLC “Consulting Publishing Company “Business Perspectives”



NUMBER OF REFERENCES

44



NUMBER OF FIGURES

5



NUMBER OF TABLES

7

© The author(s) 2022. This publication is an open access article.



BUSINESS PERSPECTIVES



LLC "CPC "Business Perspectives"
Hryhorii Skovoroda lane, 10,
Sumy, 40022, Ukraine
www.businessperspectives.org

Received on: 20th of July, 2022

Accepted on: 14th of September, 2022

Published on: 19th of September, 2022

© Volodymyr Mishchenko, Svitlana Naumenkova, Andrii Grytsenko, Svitlana Mishchenko, 2022

Volodymyr Mishchenko, Doctor of Economics, Professor, Head of the Sector of Digital Economy Institute for Economics and Forecasting of the NAS of Ukraine, Ukraine.

Svitlana Naumenkova, Doctor of Economics, Professor, Department of Finance, Taras Shevchenko National University of Kyiv, Ukraine. (Corresponding author)

Andrii Grytsenko, Doctor of Economics, Professor, Academician of the NAS of Ukraine, Deputy Director Institute for Economics and Forecasting of the NAS of Ukraine, Ukraine.

Svitlana Mishchenko, Doctor of Economics, Professor, Department of Financial Technologies and Consulting, Ivan Franko National University of Lviv, Ukraine.



This is an Open Access article, distributed under the terms of the [Creative Commons Attribution 4.0 International license](https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

Conflict of interest statement:

Author(s) reported no conflict of interest

Volodymyr Mishchenko (Ukraine), Svitlana Naumenkova (Ukraine),
Andrii Grytsenko (Ukraine), Svitlana Mishchenko (Ukraine)

OPERATIONAL RISK MANAGEMENT OF USING ELECTRONIC AND MOBILE MONEY

Abstract

The extensive use of electronic and mobile money causes additional risks, which complicates the work of electronic money issuers (EMIs) and the functioning of payment systems. The paper aims to investigate operational risk management in the process of using electronic and mobile money. A classification of operational risk types was carried out and the forms of their manifestation in payment systems using electronic and mobile money were characterized. The list of key risk indicators has been compiled to assess the operational risk factors of payment systems using mobile and electronic money; a classification of costs (losses) as a result of the implementation of operational risk events is proposed, dividing them into direct and indirect. Based on the statistics of the International Monetary Fund and the National Bank of Ukraine, the use of electronic and mobile money in certain countries of the world is analyzed. The results on the intensity of electronic money use are presented, and the value of the electronic money multiplier in Ukraine is calculated. To improve operational sustainability of EMIs, a general scheme for organizing the operational risk management process in payment systems using electronic and mobile money is presented. Particular attention is paid to the regulatory and supervisory measures aimed at supporting the operational sustainability of EMIs and payment systems under their control. The issues discussed in this paper are relevant for the debate directed at the implementation of balanced approaches to operational risk management in the process of using electronic and mobile money in developing and emerging economies.

Keywords

electronic money, mobile money, electronic money issuers, operational risk, financial regulation

JEL Classification

E42, G20, G35

INTRODUCTION

Recently, due to the spread of remote work, e-commerce, receiving social benefits and social assistance in connection with the COVID-19 pandemic, forced migration, electronic and mobile money are increasingly being used. The main advantages of using such money are high speed and low cost of money transfer, convenience, accessibility, personalization and anonymity.

Non-banking financial and non-financial organizations are increasingly entering the payment services market; various forms of external influence are intensifying, from natural disasters to cybercrime. All this contributes to an increase in the level of EMI riskiness and the functioning of payment systems.

The main sources of operational risk in payment systems using electronic or mobile money are information and communication technologies, hardware, software, communication networks and related human activities, which require a significant increase in the level of protection and necessitate the use of appropriate risk management methods and tools.

Some experience has already been gained in managing operational risk arising in payment systems using electronic or mobile money. However, there is some uncertainty regarding the identification of operational risk by type, the use of methods and indicators to assess the impact of operational risk on the activities of issuers and users of electronic payment instruments. In addition, the lack of unified internationally agreed approaches to the regulation and supervision of the activities of non-banking EMIs and related payment systems hinders the process of improving operational risk management.

1. LITERATURE REVIEW

Key concepts and recommendations for all stakeholders on the digital security risk are covered in the OECD Recommendation and Companion Document (OECD, 2015). Operational risk management in payment systems based on the use of electronic and mobile money is most often studied in the scientific literature in the context of the overall risk management of a company or payment system. In EU countries, the issuance of electronic money is regulated by Directive 2009/110/EC (EC, 2009). Authorities issuing licenses to electronic money issuers should be guided by this document. A general requirement for the risk management system is the need to ensure its effective integration into a single mechanism for managing a company as a whole (COSO, 2017).

The issues of the economic nature, causes and forms of operational risk associated with the use of electronic and mobile money have been studied in detail by Onyiriuba (2016), Wonglimpiyarat (2016). Mobile money opens new opportunities for financially excluded adult (Demirgüç-Kunt et al., 2017). Suri (2017) described the future of mobile money in developing economies. Ahmad et al. (2020) notes the distinction between m-money and m-banking. There are different approaches to identifying the types and forms of manifestation of operational risk. So, Iivariinen et al. (2003) consider information, technological, administrative and criminal risks to be the main types of operational risk inherent in payment systems. Greenacre and Buckley (2015) list provider failure, EMI illiquidity, and fraud as types of operational risk. Dobler et al. (2021) distinguish five types of operational risk, namely, internal and external fraud, cyber risk, agency risk, business and investment risk, including the failure of a bank that serves an EMI. Gutierrez and Jeffrey (2006) distinguish information risk among the types of operational risk and determine the conditions for ensuring a company's information security.

Chernobai et al. (2021) point to the dependence of the level of operational risk on the complexity of a company's business model. The influence of operational risk on other types of risks inherent in payment systems, in particular liquidity risk, is being actively studied (Merrouche & Schanz, 2010). Varga et al. (2021) draw attention to potential of reputational risk and loss.

At the same time, it should be noted that most researchers in the process of assessing the risks of EMIs' activities, in particular operational ones, are guided by the approaches developed by international organizations (Clark & Ebrahim, 2022). For example, the Basel Committee on Banking Supervision identifies seven types of operational risk in relation to banking activities (BCBS, 2011). The Bank for International Settlements has proposed new principles for the operational sustainability of banks, taking into account the rapid pace of information technology development and the COVID-19 pandemic (BIS, 2020). The OECD Digital Economy Outlook 2020 reviews trends in digital security risk and digital security policies (OECD, 2020a).

A separate area of research is the management of privacy risk in digital payment systems that may result from cyber-attacks or other types of external interference (Netscout, 2019; Li & Liu, 2021). OECD report "The Role of Public Policy and Regulation in Encouraging Clarity in Cyber Insurance Coverage" examines the differences in the coverage of cyber losses and what types of losses are covered (OECD, 2020b). Akanfe et al. (2020) developed a methodology for calculating the privacy risk index and substantiated methods for ensuring privacy, which include the need to develop a company's privacy policy and comply with regulatory requirements.

Gonzalez (2014) explored the issue of online risk management by strengthening organizational and technical support for the security of mobile

devices and social networks. Haberly et al. (2019) assessed the impact of digital platforms on risk management. Del Gaudio et al. (2021) described the role of new ICTs in reducing operational risk and improving EMI stability.

Rubio et al. (2021) investigated the features of operational risk monitoring. Akanfe et al. (2020) focus on improving methods for measuring, quantifying and qualitatively assessing operational risk. To estimate the real losses from operational risk, Bonet et al. (2021) use the scenario analysis method. Barakat et al. (2014) propose to carry out such an assessment taking into account the level of information asymmetry. The socio-economic aspect of operational risk management, related to its impact on the level of financial inclusion, deserves attention (Naumenkova, 2015; Lashitew et al., 2019).

A separate line of research is the identification of sources and forms of compensation for losses in the event of operational risk realization. According to Aron (2018) the channels through which mobile money can affect the economy are many and not well-understood. Along with proposals for risk insurance and the creation of special innovation funds (Mishchenko et al., 2021), there are various proposals related to profit compensation (Del Gaudio et al., 2021) and the formation of EMI capital buffers.

The vast majority of authors quite rightly believe that operational risk management in EMI activities should be based on the general recommendations of national regulators for managing the risks of the functioning of payment systems (Kellogg, 2003; Ng et al., 2021). To prevent risks, almost all EMIs set limits on the amount of transactions. Microloans are provided depending on the amount of turnover of funds in a user's electronic account (IMF, 2021).

Given the importance of EMIs and the payment systems they use, there is a growing need for unified regulation and supervision of EMIs (BIS, 2012; OECD, 2020b; Ehrentraud et al., 2021). Katusiime (2021) emphasize the need to develop clear rules and procedures in order to reduce losses of electronic and mobile money users. It should be noted that international financial organizations and regulators are stepping up work on developing prin-

ciples and improving the methodology for regulating and supervising the circulation and use of electronic and mobile money. Thus, the methodological approaches of the Bank for International Settlements (BIS, 2012) to organizing the supervision of electronic money as a payment system (the PFMI Principles) and the PISA rules, a system for the supervision of the use of electronic payment instruments developed by the European Central Bank (ECB, 2021), should not be overlooked.

2. AIMS AND METHODS

The paper aims to study operational risk management in the process of using electronic and mobile money. The study is based on the generalization of the results of using electronic and mobile money in certain countries of the world based on IMF data on the volume and structure of payments for 2015–2021. To calculate the value of the electronic money multiplier, the NBU data on the operations of Ukrainian banks with electronic money in 2014–2021 were used.

The study of operational risk management processes in the use of electronic and mobile money is based on the principles of effective operational risk management developed by the Basel Committee on Banking Supervision (BCBS, 2011); financial market infrastructure principles (BIS, 2012); COSO ERM 2017 Standards (COSO, 2017); Bank for International Settlements Operational Sustainability Principles (BIS, 2020); ECB Guidelines for Eurosystem Supervision of Electronic Payment Instruments, Schemes and Mechanisms (ECB, 2021).

According to Directive 2009/110/EC (EC, 2009), electronic money was considered to be a monetary value stored on a special electronic device, accepted as a means of payment by persons other than the issuer, and which is a claim on its issuer, while mobile money was considered as a form of electronic money, a feature of which is the service of payments using mobile phones or the Internet. At the same time, it was taken into account that, according to the PISA rules (ECB, 2021), electronic and mobile money are types of electronic payment instruments that allow the transfer of value or the fulfillment of payment obligations between users.

Also, the key difference in the use of electronic and mobile money associated with the legal status and forms of EMIs, in particular, with the peculiarities of regulation and supervision of their activities, is considered.

3. RESULTS AND DISCUSSION

The use of digital and mobile money as electronic payment instruments remains at a high level and continues to spread, covering new financial services markets. India, Indonesia, Italy, and Japan have become leaders in the use of electronic money. The largest number of payments using electronic money per inhabitant is observed in Japan and Indonesia, and the average value is in Italy, the USA, Japan, Singapore, and Switzerland. At the same time, the share of e-money payments in value of card and electronic payments in these countries in 2020 ranges from 11.77% in Japan

to 28.41% in Indonesia. However, in many of the most economically developed countries such as France, Germany, the Netherlands and Spain electronic money is not widely used, and its share in the value of card and e-money payments varies between 0.02 and 0.35% (Table 1).

Compared to the use of e-money, the scope of mobile money is much wider and covers the vast majority of African countries and a significant number of countries in Asia and Latin America. Thus, in African countries, the number of registered mobile money accounts in 2020 amounted to more than USD 500 million, and the total amount of transactions made was USD 495 billion, which is equal to approximately 18-19% of the GDP of all countries of the continent (Coulibaly, 2021).

Mobile money is most widely used in East African countries such as Kenya, Mozambique, Rwanda, Uganda, Zambia, and Zimbabwe (Table 2).

Table 1. Relative importance of e-money payments in selected countries of the world in 2015 and 2020 (in value of card and e-money payments, %)

Source: Calculated based on BIS Statistics (2020).

Country	Card and e-money payments							
	By card with a debit function		By card with a delayed debit function		By card with a credit function		E-money payments	
	2015	2020	2015	2020	2015	2020	2015	2020
Argentina	32.35	39.88	n.a.	n.a.	67.65	51.45	0,00	8.67
Australia	43.85	56.22	n.a.	n.a.	56.15	43.14	n.a.	0.64
Belgium	78.52	81.73	14.59	10.25	6.45	4.92	0.44	3.10
Brazil	36.65	40.34	n.a.	n.a.	63.23	57.06	0.12	2.60
Canada	34.29	36.50	n.a.	n.a.	65.71	63.50	n.a.	n.a.
France	54.87	65.99	23.64	20.53	21.41	13.36	0.09	0.12
Germany	65.18	73.46	32.26	24.22	2.36	2.06	0.21	0.26
India	33.67	43.97	5.03	1.04	50.98	42.00	10.33	13.00
Indonesia	43.04	39.49	n.a.	n.a.	55.88	32.10	1.08	28.41
Italy	59.20	53.32	n.a.	n.a.	31.06	29.80	9.74	16.89
Japan	1.40	2.61	n.a.	n.a.	90.19	85.62	8.41	11.77
Korea	19.56	21.54	n.a.	n.a.	80.31	77.79	0.12	0.67
Mexico	54.22	60.99	n.a.	n.a.	45,78	39,01	n.a.	n.a.
Netherlands	88.61	88.83	11.38	11.15	n.a.	n.a.	0.02	0.02
Russia	89.35	94.10	n.a.	n.a.	6.99	4.03	3.66	1.87
Saudi Arabia	84.81	89.81	n.a.	n.a.	15.19	10.19	n.a.	n.a.
Singapore	39.12	37.27	n.a.	n.a.	57.62	60.70	3.27	2.03
Spain	51.63	64.07	48.37	35.58	n.a.	n.a.	n.a.	0.35
Sweden	72.97	76.20	4.45	3.04	22.58	20.76	n.a.	n.a.
Switzerland	54.90	57.77	n.a.	n.a.	43.19	39.28	1.91	2.96
Turkey	6.99	15.72	n.a.	n.a.	92.86	83.53	0.14	0.74
United Kingdom	73.50	80.09	4.42	2.84	22.08	17.06	n.a.	n.a.
United States	42.45	42.14	n.a.	n.a.	54.67	54.66	2.89	3.20

Table 2. Number of mobile money transactions per 1,000 adult citizens in selected countries of the world in 2015–2021, units

Source: Compiled by the authors based on IMF data (2021).

Country	Card and e-money payments							
	By card with a debit function		By card with a delayed debit function		By card with a credit function		E-money payments	
	2015	2020	2015	2020	2015	2020	2015	2020
Argentina	32.35	39.88	n.a.	n.a.	67.65	51.45	0.00	8.67
Australia	43.85	56.22	n.a.	n.a.	56.15	43.14	n.a.	0.64
Belgium	78.52	81.73	14.59	10.25	6.45	4.92	0.44	3.10
Brazil	36.65	40.34	n.a.	n.a.	63.23	57.06	0.12	2.60
Canada	34.29	36.50	n.a.	n.a.	65.71	63.50	n.a.	n.a.
France	54.87	65.99	23.64	20.53	21.41	13.36	0.09	0.12
Germany	65.18	73.46	32.26	24.22	2.36	2.06	0.21	0.26
India	33.67	43.97	5.03	1.04	50.98	42.00	10.33	13.00
Indonesia	43.04	39.49	n.a.	n.a.	55.88	32.10	1.08	28.41
Italy	59.20	53.32	n.a.	n.a.	31.06	29.80	9.74	16.89
Japan	1.40	2.61	n.a.	n.a.	90.19	85.62	8.41	11.77
Korea	19.56	21.54	n.a.	n.a.	80.31	77.79	0.12	0.67
Mexico	54.22	60.99	n.a.	n.a.	45.78	39.01	n.a.	n.a.
Netherlands	88.61	88.83	11.38	11.15	n.a.	n.a.	0.02	0.02
Russia	89.35	94.10	n.a.	n.a.	6.99	4.03	3.66	1.87
Saudi Arabia	84.81	89.81	n.a.	n.a.	15.19	10.19	n.a.	n.a.
Singapore	39.12	37.27	n.a.	n.a.	57.62	60.70	3.27	2.03
Spain	51.63	64.07	48.37	35.58	n.a.	n.a.	n.a.	0.35
Sweden	72.97	76.20	4.45	3.04	22.58	20.76	n.a.	n.a.
Switzerland	54.90	57.77	n.a.	n.a.	43.19	39.28	1.91	2.96
Turkey	6.99	15.72	n.a.	n.a.	92.86	83.53	0.14	0.74
United Kingdom	73.50	80.09	4.42	2.84	22.08	17.06	n.a.	n.a.
United States	42.45	42.14	n.a.	n.a.	54.67	54.66	2.89	3.20

An analysis of the use of mobile money shows their high popularity among low-income citizens who do not have a bank account or other access to the financial system. Today, EMIs, in cooperation with official financial institutions, telephone and trading companies, are expanding their activities and, in addition to payment services, can provide users with a wider range of financial services such as lending, savings, insurance, etc. The use of mobile money is also increasing due to the COVID-19 pandemic, the spread of remote work, online trading, receiving social benefits, social assistance, etc. Thus, during 2015–2021, balances on the wallets of mobile money users grew at an extremely high rate in Zimbabwe, Zambia, Guinea, Cameroon and Myanmar (Table 3).

The activity of an EMI, as a payment system organizer, involves the issuance of electronic or mobile money and their storage on transaction accounts, making payments between electronic wallets through a telecommunications network using a mobile phone or the Internet, manag-

ing user funds, as well as managing an agent network.

One of the most well-known mobile money systems is the Kenyan payment system M-Pesa, created by the mobile operator Safaricom in 2007. Today, this system has more than 6.5 million users, making several million transactions daily, which provides the operator with about 13% of the profit.

Based on the M-Pesa system, similar payment systems have been created in South Africa, Lesotho, Mozambique, Tanzania, Afghanistan and many other countries. In addition to M-Pesa, mobile money systems such as MTN Money in Uganda, Orange Money in Côte d'Ivoire, MoMo in South Africa and others are widely known. Therefore, in 2022, under the auspices of the Bank of Tanzania and with the participation of three banks and two mobile money platform operators, a new Tanzania Instant Payment System (TIPS) was created, combining the Tanzanian mobile payment market into a single system.

Table 3. The total amount of outstanding balances on active mobile money accounts in 2015–2021 (in millions of national currency)

Source: Compiled by the authors based on IMF data (2021).

Country	2015	2016	2017	2018	2019	2020	2021
Afghanistan	200	435	707	559	696	n.a.	n.a.
Armenia	124	302	678	1,158	1,281	2,707	n.a.
Bangladesh	10,695	17,861	27,285	27,534	40,930	58,342	70,871
Botswana	44	48	81	108	142	286	532
Cameroon	4,656	22,354	53,129	90,887	109,607	136,067	n.a.
Ghana	548	1,257	2,321	2,634	3,634	6,980	n.a.
Guinea	33,153	9,270	251,500	468,370	721,277	1,115,725	1,404,826
India	576	3,884	14,054	26,957	26,320	28,382	n.a.
Indonesia	737,786	982,360	2,421,094	4,033,008	6,142,712	7,893,321	n.a.
Madagascar	78,068	112,514	161,483	85,241	195,657	231,948	n.a.
Myanmar	369	603	4,797	5,735	56,267	n.a.	n.a.
Pakistan	8,827	11,717	21,139	23,678	28,770	51,671	n.a.
Panama	11,520	12,407	0	224,702	574,640	1,636,867	2,449,914
Philippines	14,372	13,831	14,629	17,343	22,420	n.a.	n.a.
Rwanda	17,023	19,865	17,446	19,960	28,532	67,151	n.a.
Thailand	345	596	941	1,435	3,598	4,097	n.a.
Uganda	325,293	353,733	468,437	338,207	417,594	571,362	n.a.
Zambia	46	96	267	874	1,218	2,256	3,165
Zimbabwe	89	130	325	542	1,830	5,102,815	n.a.

Since operational risk has a complex form of manifestation and is inherent in all aspects of EMI activities, *segregation* procedures are carried out to prevent the spread of EMI risks, that is, the separation of user funds from EMI assets in order to protect them in the event of an issuer's bankruptcy and to satisfy creditors' claims.

In most countries, segregation is carried out based on the introduction of the following measures:

- creation of trusts for trust management (Afghanistan, Bangladesh, Kenya, Lesotho, Liberia, Malawi, Myanmar, Namibia, Rwanda, Tanzania, Zambia);
- conclusion of fiduciary agreements (Latin American countries);
- use of escrow accounts (India);
- introduction of legal restrictions: electronic and mobile money of users are legally separated from EMI assets (Brazil, Chad, the Philippines).

In addition, to prevent risks, almost all EMIs set limits on the number of transactions. For example, the M-Pesa system sets absolute limits on one-time

and daily fund transfers. A one-time transfer can be made up to 70,000 shillings (approximately 700 USD), and the one-day amount must not exceed 140,000 shillings. In South Africa, the amount of the money transfer depends on the account class established by an EMI (for a standard class account, no more than 5 thousand rands, and for a premium class, no more than 25 thousand rands). Microloans in both systems are provided depending on the amount of turnover of funds in a user's electronic account (IMF, 2021).

In Ukraine, electronic money has been used since 2005, and its issuers are exclusively banks. In 2014–2021, the volume of issued electronic money increased by 3.0 times, the number of electronic wallets decreased by 31.8%, and the volume of transactions increased by 7.1 times. It should also be noted that the intensity of using electronic money was the highest in 2020 and 2021, when their multiplier equaled 321.7 and 272.5, respectively (Figure 1).

However, the use of electronic money in Ukraine has not received the expected distribution due to legislative restrictions on the maximum amount of funds that can be stored on electronic devices and the maximum amount of payments, as well as due to the introduction of mandatory identifi-

Source: Elaborated by the authors based on NBU data (2021).

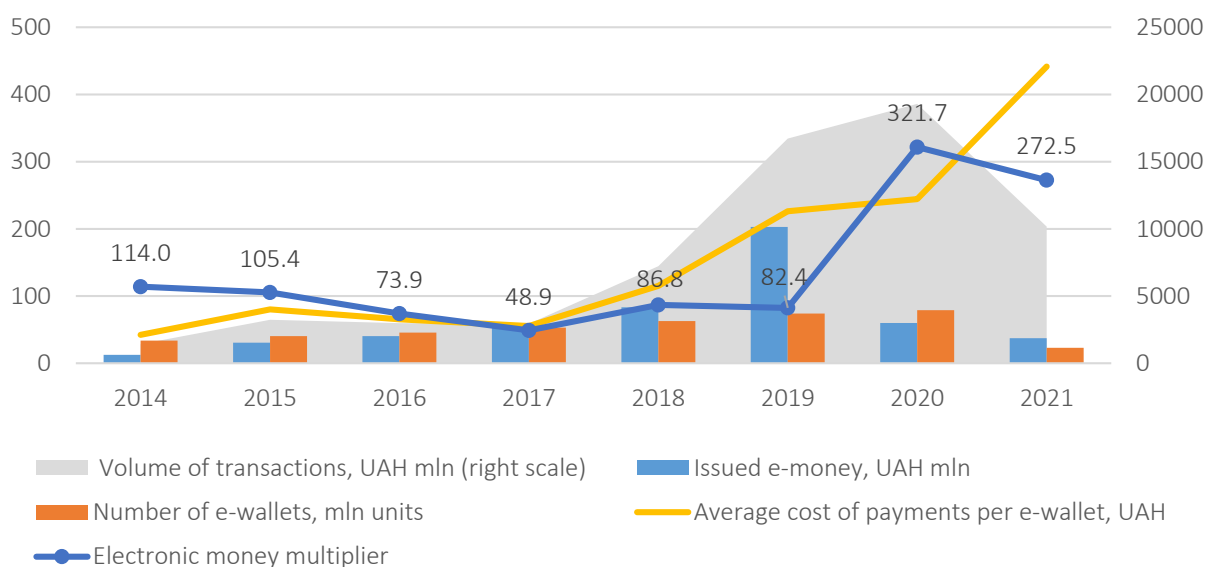


Figure 1. Issue and circulation of electronic money in Ukraine in 2014–2021

cation of e-wallet users, as a result of which the share of electronic money payments in the total volume of payment transactions in 2021 was only 0.38%. Given the high level of restrictions on using electronic money in Ukraine, the main sources of operational risk in payment systems can be information and communication systems and external interference.

The results of the analysis indicate that the use of electronic money in Ukraine remains relevant and may receive new development. Given the situation in the Ukrainian energy sector, the risks and threats caused by full-scale war, there is a need to analyze the readiness of Ukraine to generate sustainable and reliable energy for digital development (Naumenkova et al., 2022).

Summarizing the above, the operational risk of payment systems using electronic or mobile money can be defined as the possibility of loss or other losses due to deficiencies in the functioning of information and technological systems, communication channels, EMI internal processes and policies, errors of personnel, users or agents, the actions of intruders, or as a result of the external factors.

It should be noted that the *operational risk management system is a set of methods for analyzing and neutralizing risk factors, combined into a sin-*

gle mechanism for assessing, monitoring and corrective actions to maintain the operational sustainability of EMIs.

Therefore, the operational risk management process is subordinated to the solution of an important task such as ensuring the operational stability of EMIs, which allows us to consider it as a component of a company's management as a whole and increase its stability.

With this in mind, the operational risk management process should be primarily aimed at maintaining the operational sustainability of EMIs and preventing the occurrence of critical risks (Appendix A).

This process consists of the following steps:

- risk diagnostics, including qualitative analysis (identification, categorization and prioritization) and quantitative analysis of operational risks;
- risk management assessment: determination of key risk indicators (KRIs) and development of risk response measures;
- risk monitoring: formation of relevant departments, analysis of response measures and adjustment of the risk management program.

Let us consider in more detail the main stages of the EMI operational risk management process.

First of all, it is necessary to correctly determine the operational risk in payment systems using electronic and mobile money. Given the recommendations and guidelines of the IMF, BIS, BCBS, ECB, EBA and the central banks of individual countries, five types of operational risk can be distinguished, the most relevant today for payment systems operating based on the use of electronic and mobile money (Table 4).

Each of the identified types of operational risk has its own factors of occurrence and forms of manifestation, which expose the EMI payment system to financial and other types of losses. Table 4 describes in detail the features and forms of manifestation of certain types of operational risk in electronic and mobile money payment systems.

Therefore, the key elements of identifying the risk of using electronic and mobile money should be the identification, registration and description of risk events, followed by an assessment of the

Table 4. Characteristics of operational risk manifestation forms in electronic and mobile money payment systems

Risk type	Risk events	Registration and description of events that may cause the risk to realize (factors of occurrence)
1. Information security risk (including cyber risk)	Termination of activity or threat to the functioning of information, communication and technological systems, which makes it impossible or limits the performance of transactions. Damage or destruction of assets as a result of emergencies	<ul style="list-style-type: none"> • Unauthorized impact on information systems, software and technical infrastructure; • distortion or disclosure of information assets, termination of operation or damage to information systems and communication networks; • destruction, theft or disclosure of confidential information, seizure of funds or information assets, extortion and other forms of illegal influence; • intentional actions of EMI employees or third parties using information technologies aimed at information systems, software, communication networks and information assets in order to violate protection systems and create threats to information security; • natural disasters, man-made disasters, military conflicts, terrorism, accidents, vandalism
2. Information risk	Preventing the operation of information systems. Leakage of information and its use contrary to the interests of EMI and users	<ul style="list-style-type: none"> • Violations in the operation of software, hardware, communication systems and infrastructure; • loss of physical media containing confidential information; • errors of specialists when working with IT systems; • unauthorized access to information systems using malicious software that violates the integrity, availability and confidentiality of information
3. Risk of errors in management processes	Violation of management processes, untimely or poor-quality performance of management functions and provision of services	<ul style="list-style-type: none"> • - Lack of provisions, procedures, management structures; • - low level of management organization, lack of interaction of individual departments; • - shortcomings in the system of control and monitoring of operational risk events; • - irregular reconciliation of balance sheet, accounting, reporting, errors in accounting and reporting
4. Risk of user errors	Violation of disclosure requirements, embezzlement, fraud	<ul style="list-style-type: none"> • Errors in user identification, in the use of technical means, in data entry and storage; • violation of the regulations or false interpretation of the terms of transactions; • legalization (laundering) of proceeds from crime; • exceeding the established limits on transactions; unauthorized access to electronic wallets; • loss (theft) of funds
5. Risk of errors in managing the network of agents	Violation of fiduciary obligations. Reducing the number of clients. Conflicts with users	<ul style="list-style-type: none"> • Unintentional errors, intentional actions or omissions of EMI agents and other related persons; • failure to comply with the user identification requirements, violation of the disclosure conditions or improper use of confidential information, failure to provide or provision of incomplete information to users; • unlawful collection of commissions, violation of the requirements of the instructions, fiduciary obligations; • erroneous interpretation of the terms of operations; • claims of users; • non-fulfillment of reporting obligations, errors in reporting

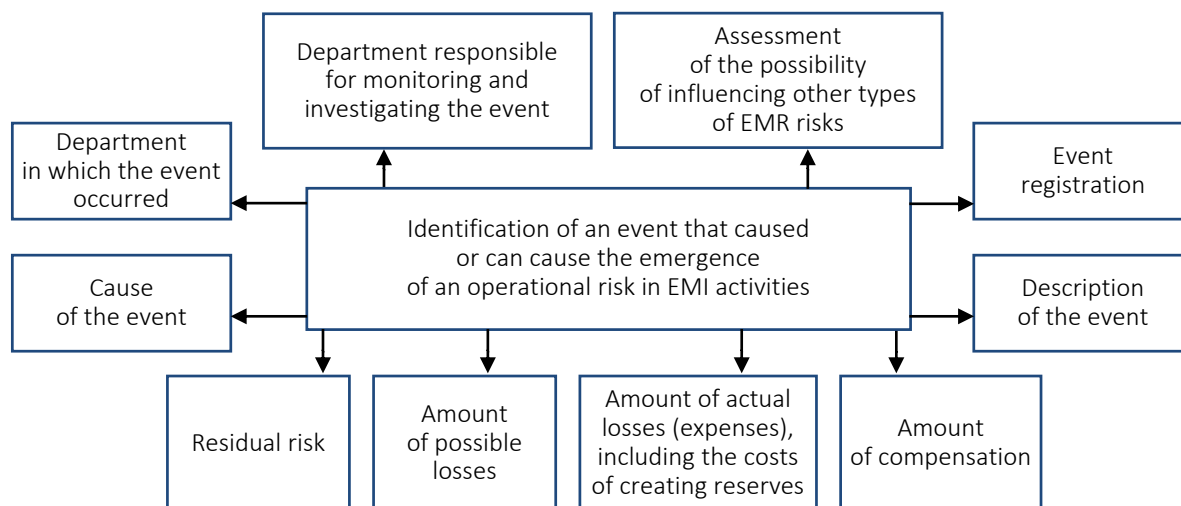


Figure 2. Scheme for organizing the identification and documentation of events that have resulted in operational risk

amount of losses (damages) and determining the potential impact on other types of risks (Figure 2).

To prioritize risks, information about operational risk events and their impact on business results, accumulated in the EMI database, allows you to determine the probability of realization and the potential level of losses. Usually, more complex types of risks are less likely to materialize, but the losses from them can be very large. And, on the contrary, simpler types of risk have a higher probability of realization, although they are characterized by a lower level of losses (Table 5).

Table 5. Estimation of realization probability, potential loss levels and risk exposure as a result of the impact of certain types of EMI activities' operational risk

Operational risk type	Probability of realization	Potential loss level	Risk exposure
Information security risk (including cyber risk)	3	5	15
Information risk	3	3	9
Risk of errors in management processes	3	3	9
Risk of user errors	5	1	5
Risk of errors in managing the network of agents	5	1	5

Note: Rating scale. Risk realization probability: low – 1; medium – 3; high – 5. Potential risk of loss: low – 1; medium – 3, high – 5.

An important step in diagnosing the priority of operational risks of payment systems using electronic and mobile money is to ensure the continuity of transfers and payments, to prevent the occurrence of critical risks and to ensure the operational sustainability of the payment system using electronic payment instruments.

With this in mind, special attention should be paid to the following indicators:

- *recovery point objective (RPO)*, the maximum time during which the system can lose its critical functions; and
- *recovery time objective (RTO)*, the time required to restore information systems and processes after a shutdown to normal operation conditions.

Quantitative risk analysis is a cost assessment of the consequences of their implementation and potential impact on all participants in the payment system. Quantitative analysis is carried out after qualitative analysis (identification, prioritization and categorization). Quantitative risk analysis allows you to more accurately determine the list of risk response measures, including the use of appropriate tools to protect against possible losses if risks materialize.

Summarizing EMI operation experience made it possible to identify and group the main types of

potential losses, shortfalls in planned income or the occurrence of other things as a result of implementing operational risk events (Table 6).

Table 6. Classification of losses (damage) as a result of operational risk events

Direct losses (represented in accounting)	Indirect losses (not represented in accounting)
<ul style="list-style-type: none"> • Decrease in the value of a company's assets; • early write-off of tangible, intangible and financial assets; • loss of user funds; • cash payments to customers and counterparties in order to compensate for losses caused through the fault of third parties; • cash payments to employees as compensation for losses caused to them by the company, out of court; • losses from erroneous payments; • expenses related to court decisions; • fines imposed by executive authorities; • costs to restore activities or eliminate the consequences of a risky event; • financial losses due to unfavorable transactions for the company 	<ul style="list-style-type: none"> • Decrease in the market value of a company; • lost income due to suspension of activities or non-execution of transactions due to a risk event; • shortfall in income as a result of non-fulfillment of obligations or execution of unprofitable agreements; • lost income as a result of reduced quality of services; • lost income due to leakage, loss or distortion of information; • fines of state and judicial bodies; • resolutions, acts of state bodies not related to the payment of fines; • temporary unavailability of user funds; • loss of customers

To ensure the emergence of critical EMI risks, it is important to substantiate the system of *key risk indicators (KRI)*, which characterize the change in the level of operational risk and can be used for early detection and quantitative assessment of the negative impact of risk factors. It is worth noting that such a list of KRIs should be determined by each company independently, depending on the working conditions and accumulated experience in risk management.

This study proposes a list of KRIs for assessing the operational risk factors of payment systems using mobile and electronic money:

- 1) the ratio of the number of failures in the execution of transactions to the total number of

transactions performed during a certain period of time, %;

- 2) the share of transactions made over a certain period of time with signs of internal and external fraud in the total number of transactions for the same period, %;
- 3) the share of transactions made during a certain period of time in violation of the established limits in the total number of transactions for the same period, %;
- 4) duration of termination (restriction) of the system due to technical or technological violations, minutes;
- 5) duration of system recovery after the termination of activities in the case of a risk event, minutes;
- 6) time interval between two consecutive events that led to the termination (limitation) of the functioning of the payment system, characterizing the continuity of its work;
- 7) the number of cases of unauthorized access to users' electronic wallets for a certain period of time;
- 8) amount of fines paid and compensation for losses as a percentage of operating income, %;
- 9) frequency of change (turnover) of EMI agents and mediators during a certain period of time, %.

The level of operational risk management depends on the availability of tools for identifying, measuring, monitoring and controlling risk, the methodology for calculating actual and potential losses, as well as the procedure for monitoring the functioning of the EMI-controlled payment system. Based on the analysis of the experience of managing payment systems, a scheme for organizing the operational risk management process for systems using electronic and mobile money can be proposed (see Figure 3).

To increase the level of operational risk management in a payment system using electronic or mobile money, a system of measures (Table 7) is proposed.

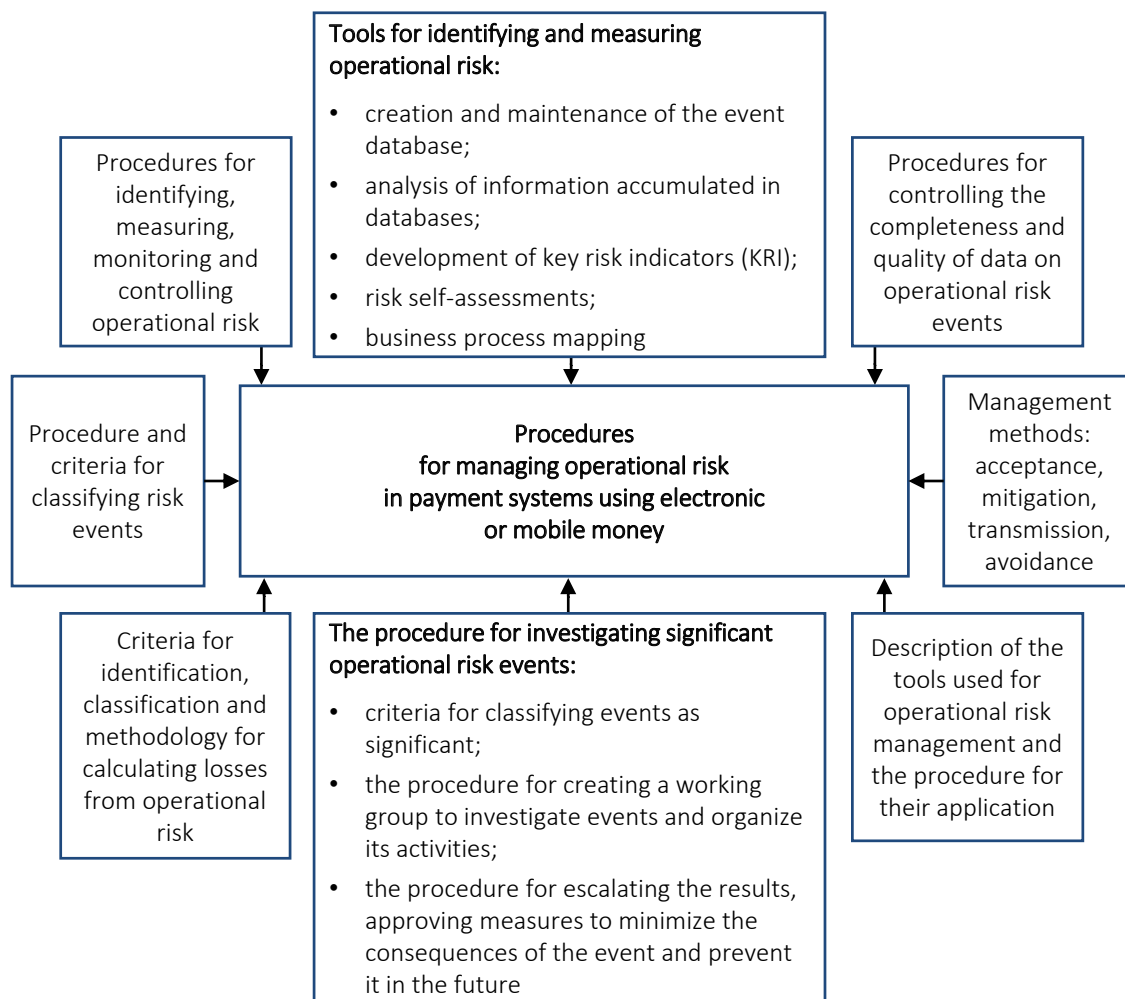


Figure 3. Scheme for organizing the operational risk management process in payment systems using electronic and mobile money

Along with the methods used by EMIs to assess and manage operational risk, the formation of a general regulatory and prudential landscape of their activities is important, since most of these companies are not subject to the prudential requirements of payment market regulators. As noted above, this issue becomes especially relevant due to the fact that large payment systems created by EMIs, due to significant volumes of transactions and a large number of participants, can be of systemic importance and significantly affect the stability of the entire financial system of a country.

In this regard, the introduction by the payment market regulators of effective regimes for regulating and supervising the activities of EMIs in order to ensure their stable functioning on the market and strengthening mechanisms for protecting users' funds becomes an urgent practical task. Such

regulation regimes can be considered as indirect methods of maintaining the operational sustainability of EMIs. Studying the experience of individual countries regarding the regulation and supervision of EMI activities allows generalizing the prudential approaches of money and payment market regulators aimed at reducing risks and supporting the stable functioning of payment systems using electronic and mobile money in such areas (Figure 4).

It is important to note that the high growth rates of mobile money use, the increase in the number of users, and the presence of a wide network of agents can expose EMIs to additional risks and contribute to an increase in the level of operational risk. *With the increasing use of mobile money, e-wallet holders can use a variety of online services with different levels of protection, and therefore*

Table 7. Measures to prevent and limit the impact of operational risk factors to maintain proper operational sustainability of EMIs

Areas	Characteristics of measures
Compliance with information security and operational reliability requirements	<ul style="list-style-type: none"> • implementation of information security standards; • periodic assessment of the security of software, services and apps; • periodic review of internal regulations, provisions and instructions for information security; • use of automated means of responding to signs of cyber-attacks; • prevention of unauthorized access; • differentiation of access to systems and data; • copying and archiving of data and information resources; • tightening of technological requirements for the transfer of funds and payments; • improvement of systems and technologies to protect software and hardware systems and information
Ensuring business continuity	<ul style="list-style-type: none"> • periodic software updates; • reservation of software and technical resources; • creation of reserve computing capacities; • regular testing of information systems and hardware and software systems
Strengthening monitoring and control of operational risk	<ul style="list-style-type: none"> • use of reliable user identification methods; • improvement of methods for identifying and preventing operational risk; • strengthening control over compliance with established rules and procedures; • monitoring and timely response to cyber-attacks; • regular stress testing of operational risk events based on the scenario analysis method
Organizational and management measures to minimize the effects of operational risk	<ul style="list-style-type: none"> • organization of a monitoring and control system for potential vulnerabilities; • improvement of the rules and procedures of activity and organizational and management structure; • timely provision of relevant information to users; • insurance in case of operational risk implementation; • creation of reserves to eliminate the consequences of operational risk implementation

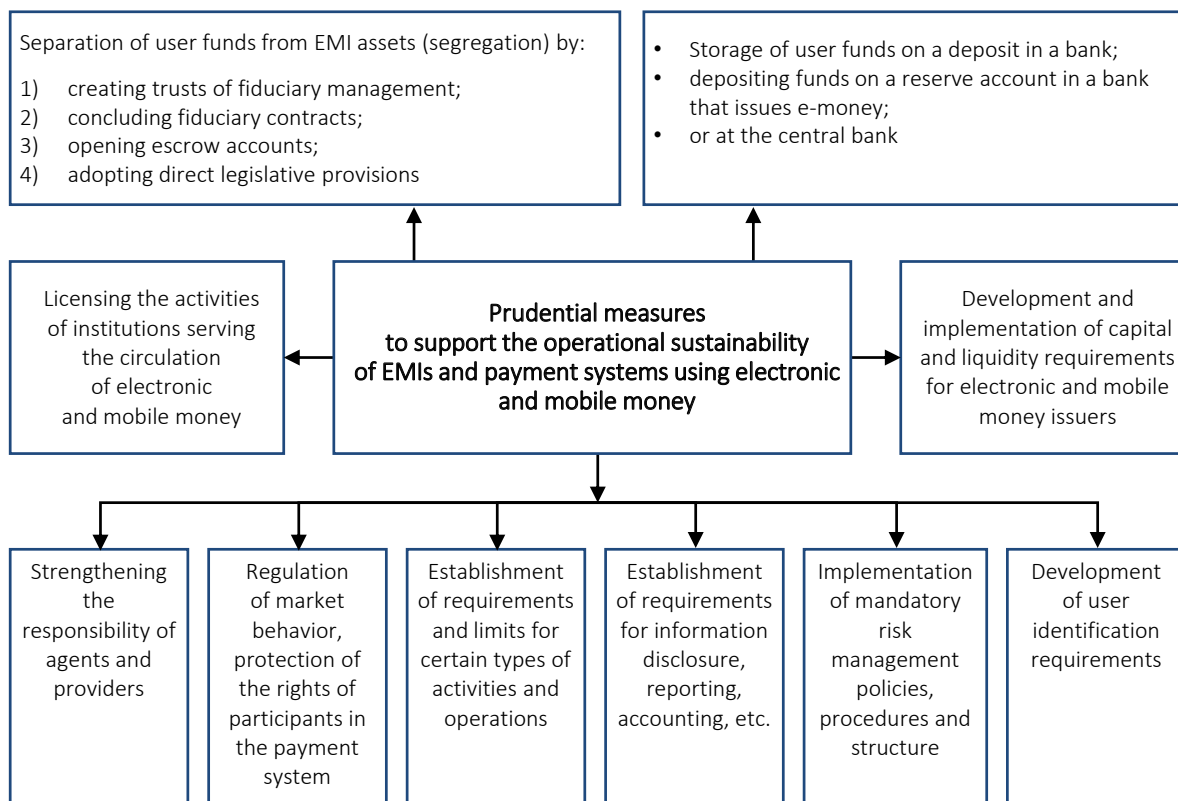


Figure 4. A system of regulatory and prudential measures aimed at supporting the operational sustainability of EMIs and payment systems under their control

raising the level of risk can happen automatically, regardless of users or EMIs. Under such conditions, risks can become systemic and pose a threat to the entire financial system of a country.

The formation of a common regulatory and prudential landscape of EMIs should be based on a

system of regulatory and prudential measures aimed at supporting the operational sustainability of EMIs and payment systems controlled by them. The proposed measures will help ensure the stable functioning of EMIs, taking into account the interests of the state and users of electronic and mobile money.

CONCLUSION

This paper discusses the operational risk management in the process of using electronic and mobile money. The calculations obtained indicate an increase in the intensity of the use of electronic money in developing countries and Ukraine. Disclosing the content of operational risk and the forms of its manifestation in payment systems using electronic or mobile money, it is emphasized that operational risk management should be subordinated to the solution of the main task such as ensuring the operational sustainability of EMIs. In the absence of unified approaches to managing operational risk of electronic money issuers, developing countries try to independently develop guidelines and recommendations, most often based on segregation measures and restrictions on the volume of transactions.

To maintain an appropriate level of operational risk management and protect against the occurrence of critical of electronic money issuers risks, a list of key risk indicators has been compiled to assess the operational risk factors of payment systems using mobile and electronic money. Based on the results of the study, a classification of costs (losses) as a result of the implementation of operational risk events is proposed, dividing them into direct (reflected in accounting) and indirect (not reflected in accounting). The paper presents a general scheme for managing operational risk of a payment system using electronic payment instruments in order to strengthen control over the occurrence of critical risks and maintain the operational sustainability of an EMI at an appropriate level. The scheme allows for logical and consistent work to organize and maintain the operational sustainability of an electronic money issuer in countries with fragile economies.

AUTHOR CONTRIBUTIONS

Conceptualization: Volodymyr Mishchenko, Svitlana Naumenkova, Andrii Grytsenko.

Formal analysis: Volodymyr Mishchenko, Svitlana Mishchenko.

Investigation: Volodymyr Mishchenko, Svitlana Naumenkova, Andrii Grytsenko, Svitlana Mishchenko.

Methodology: Volodymyr Mishchenko, Svitlana Naumenkova, Andrii Grytsenko.

Project administration: Svitlana Naumenkova.

Supervision: Andrii Grytsenko.

Visualization: Svitlana Naumenkova, Svitlana Mishchenko.

Writing – original draft: Volodymyr Mishchenko.

Writing – reviewing & editing: Svitlana Naumenkova, Svitlana Mishchenko.

REFERENCES

-
1. Ahmad, H. A., Green, C., & Jiang, F. (2020). Mobile Money, Financial Inclusion and Development: A Review with Reference to African Experience. *Journal of Economic Surveys*, 34(4), 753-792. <https://doi.org/10.1111/joes.12372>
 2. Akanfe, O., Valecha, R., & Rao, H. R. (2020). Assessing country-level privacy risk for digital payment systems. *Computers & Security*, 99, 102065. <https://doi.org/10.1016/j.cose.2020.102065>
 3. Aron, J. (2018). Mobile Money and the Economy: A Review of

- the Evidence. *The World Bank Research Observer*, 33(2), 135-188. <https://doi.org/10.1093/wbro/lky001>
4. Barakat, A., Chernobai, A., & Wahrenburg, M. (2014). Information asymmetry around operational risk announcements. *Journal of Banking & Finance*, 48, 152-179. <https://doi.org/10.1016/j.jbankfin.2014.06.029>
 5. BCBS. (2011). *Principles for the Sound Management of Operational Risk*. BCBS. BIS. June, 2011. Retrieved from <https://www.bis.org/publ/bcbs195.pdf>
 6. BIS. (2012). *Principles for financial market infrastructures. Committee on Payment and Settlement Systems. Technical Committee of the International Organization of Securities Commissions. April 2012*. Retrieved from <https://www.bis.org/cpmi/publ/d101a.pdf>
 7. BIS. (2020). *BIS Statistics. Payments and financial market infrastructures*. Retrieved from <https://stats.bis.org/statx/toc/CPMI.html>
 8. BIS. (2020). *Principles for operational resilience. Consultative Document. August 2020*. Retrieved from <https://www.bis.org/bcbs/publ/d509.htm>
 9. Bonet, I., Peña, A., Lochmuller, C., Patiño H. A., Chiclana, F., & Gónzaga, M. (2021). Applying fuzzy scenarios for the measurement of operational risk. *Applied Soft Computing*, 112, 107785. <https://doi.org/10.1016/j.asoc.2021.107785>
 10. Chernobai, A., Ozdagli, A., & Wang, J. (2021). Business complexity and risk management: Evidence from operational risk events in U.S. bank holding companies. *Journal of Monetary Economics*, 117, 418-440. <https://doi.org/10.1016/j.jmoneco.2020.02.004>
 11. Clark, B., & Ebrahim, A. (2022). Risk shifting and regulatory arbitrage: Evidence from operational risk. *Journal of Financial Stability*, 58, 100965. <https://doi.org/10.1016/j.jfs.2021.100965>
 12. COSO. (2017). *Enterprise Risk Management – Integrating with Strategy and Performance. Executive Summary. Committee of Sponsoring Organizations of the Treadway Commission* (June 2017 ed.). Retrieved from <https://www.coso.org/Shared%20Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf>
 13. Coulibaly, S. S. (2021). A study of the factors affecting mobile money penetration rates in the West African Economic and Monetary Union (WAEMU) compared with East Africa. *Financial Innovation*, 7, 25. <https://doi.org/10.1186/s40854-021-00238-0>
 14. Del Gaudio, B. L., Porzio, C., Sampagnaro, G., & Verdoliva, V. (2021). How do mobile, internet and ICT diffusion affect the banking industry? An empirical analysis. *European Management Journal*, 39(3), 327-332. <https://doi.org/10.1016/j.emj.2020.07.003>
 15. Demirgüç-Kunt, A., Klapper, L., & Singer, D. (2017). *Financial Inclusion and Inclusive Growth: A Review of Recent Empirical Evidence* (Policy Research Working Paper No. WPS 8040). Retrieved from <http://documents.worldbank.org/curated/en/403611493134249446/pdf/WPS8040.pdf>
 16. Dobler, M., Garrido, J., Grolleman, D. J., Khiaonarong, T., & Nolte, J. (2021). *E-Money: Prudential Supervision, Oversight, and User Protection* (Departmental Paper No. 2021/027). Retrieved from <https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2021/12/13/E-Money-Prudential-Supervision-Oversight-and-User-Protection-464868>
 17. EC. (2009). *Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC*. Retrieved from <https://eur-lex.europa.eu/eli/dir/2009/110/oj>
 18. ECB. (2021). *Eurosystem oversight framework for electronic payment instruments, schemes and arrangements*. November 2021. Retrieved from https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISAPublicconsultation202111_1.en.pdf
 19. Ehrentraud, J., Prenio, J., Boar, C., Janfils, M., & Lawson, A. (2021). *Fintech and payments: regulating digital payment services and e-money* (BIS. FSI No. 33). Retrieved from <https://www.bis.org/fsi/publ/insights33.pdf>
 20. Gonzalez, D. (2014). *Managing Online Risk: Apps, Mobile, and Social Media Security. Managing Online Risk: Apps, Mobile, and Social Media Security*. Butterworth-Heinemann (286 p.). Retrieved from <https://play.google.com/books/reader?id=fyKOAAQBAJ&pg=GBS.PR1&hl=ru>
 21. Greenacre, J., & Buckley, R. P. (2015). Using Trusts to Protect Mobile Money Customers. *Singapore Journal of Legal Studies*, 59-78. Retrieved from <https://ssrn.com/abstract=2612454>
 22. Gutierrez, C. M., & Jeffrey, W. (2006). *Minimum Security Requirements for Federal Information and Information Systems*. FIPS Publication 200. National Institute of Standards and Technology. Gaithersburg, MD 20899-8930. March 2006. Retrieved from <https://csrc.nist.gov/csrc/media/publications/fips/200/final/documents/fips-200-final-march.pdf>
 23. Haberly, D., MacDonald-Korth, D., Urban, M., & Wójcik, D. (2019). Asset Management as a Digital Platform Industry: A Global Financial Network Perspective. *Geoforum*, 106, 167-181. <https://doi.org/10.1016/j.geoforum.2019.08.009>
 24. Iivarinen, T., Leinonen, H., Lukka, M., & Saarinen, V. (2003). *Regulation and control of payment system risks – a Finnish perspective*. Bank of Finland Studies. A:106. 2003. Retrieved from <https://helda.helsinki.fi/bof/bitstream/handle/123456789/9452/110738.pdf?sequence=1&is>
 25. IMF. (2021). *Access to Macroeconomic & Financial Data*. Retrieved from <https://data.imf>.

- [org/?sk=E5DCAB7E-A5CA-4892-A6EA-598B5463A34C](http://dx.doi.org/?sk=E5DCAB7E-A5CA-4892-A6EA-598B5463A34C)
26. Katusiime, L. (2021). Mobile Money Use: The Impact of Macroeconomic Policy and Regulation. *Economies*, 9(2), 1-19. <https://doi.org/10.3390/economies9020051>
 27. Kellogg, P. (2003). *Evolving Operational Risk Management for Retail Payments* (Emerging Payments Occasional Papers Series 2003-1E) (45 p.). Federal Reserve Bank of Chicago. Retrieved from <https://www.chicagofed.org/publications/occasional-papers/2003/ops-1-e>
 28. Lashitew, A. A., van Tulder, R., & Liasse, L. (2019). Mobile phones for financial inclusion: What explains the diffusion of mobile money innovations? *Research Policy*, 48(5), 1201-1215. <https://doi.org/10.1016/j.respol.2018.12.010>
 29. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7, 8176-8186. <https://doi.org/10.1016/j.egy.2021.08.126>
 30. Merrouche, O., & Schanz, J. (2010). Banks' intraday liquidity management during operational outages: Theory and evidence from the UK payment system. *Journal of Banking & Finance*, 34(2), 314-323. <https://doi.org/10.1016/j.jbankfin.2009.07.024>
 31. Mishchenko, S., Naumenkova, S., Mishchenko, V., & Dorofeiev, D. (2021). Innovation risk management in financial institutions. *Investment Management and Financial Innovations*, 18(1), 190-202. [http://dx.doi.org/10.21511/imfi.18\(1\).2021.16](http://dx.doi.org/10.21511/imfi.18(1).2021.16)
 32. Naumenkova S., Mishchenko V., & Mishchenko S. (2022) Key energy indicators for sustainable development goals in Ukraine. *Problems and Perspectives in Management*. 20(1), 379-395. [http://dx.doi.org/10.21511/ppm.20\(1\).2022.31](http://dx.doi.org/10.21511/ppm.20(1).2022.31)
 33. Naumenkova, S. V. (2015). Financial Inclusivity: Economic Contents and the Approaches to its Assessment. *Actual Problems of Economics*, 4, 363-371. (In Ukrainian.) Retrieved from http://nbuv.gov.ua/UJRN/ape_2015_4_46
 34. NBU. (2021). *E-money transactions of Ukrainian banks*. Retrieved from https://bank.gov.ua/admin_uploads/article/PS_e-money_graf_2021.jpg?v=4
 35. Netscout. (2019). *Worldwide Infrastructure Security Report* (Issue 4). Retrieved from https://www.netscout.com/sites/default/files/2020-02/SECR_001_EN-2001_Web.pdf
 36. Ng, D., Kauffman, R. J., Griffin, P., & Hedman, J. (2021). Can we classify cashless payment solution implementations at the country level? *Electronic Commerce Research and Applications*, 46, 101018. <https://doi.org/10.1016/j.elerap.2020.101018>
 37. OECD. (2015). *Digital Security Risk Management for Economic and Social Prosperity: (OECD Recommendation and Companion Document)*. <https://doi.org/10.1787/9789264245471-en>
 38. OECD. (2020a). *Digital Economy Outlook 2020*. <https://doi.org/10.1787/bb167041-en>
 39. OECD. (2020b). *The Role of Public Policy and Regulation in Encouraging Clarity in Cyber Insurance Coverage*. Retrieved from <http://www.oecd.org/finance/insurance/The-Role-of-Public-Policy-and-Regulation-in-Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf>
 40. Onyiriuba, L. (2016). Bank Work, Employees, and Operational Risk Management in Developing Economies. In *Bank Risk Management in Developing Economies* (pp. 549-568). <https://doi.org/10.1016/B978-0-12-805479-6.00028-6>
 41. Rubio, J., Pérez, B., & Arroyo, J. (2021). Risk monitoring in Ecuador's payment system: Implementation of a network topology study. *Latin American Journal of Central Banking*, 2(3), 100039. <https://doi.org/10.1016/j.latchb.2021.100039>
 42. Suri, T. (2017). Mobile money. *Annual Review of Economics*, 9, 497-520. <https://doi.org/10.1146/annurev-economics-063016-103638>
 43. Varga, S., Brynielsson, J., & Frankea, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computers & Security*, 105, 102239. <https://doi.org/10.1016/j.cose.2021.102239>
 44. Wonglimpiyarat, J. (2016). S-curve trajectories of electronic money innovations. *Journal of High Technology Management Research*, 27(1), 1-9. <http://dx.doi.org/10.1016/j.hitech.2016.04.001>

APPENDIX A

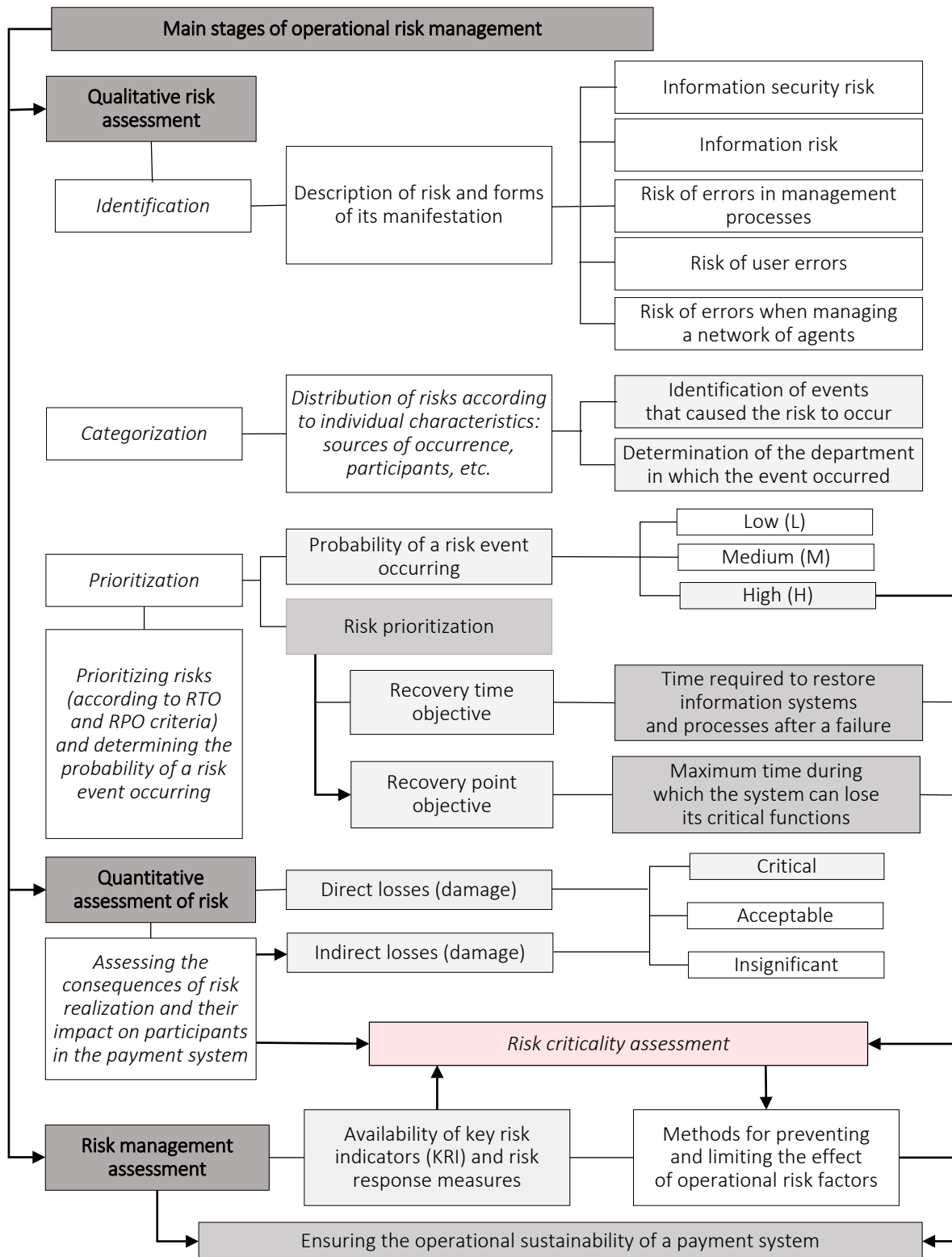


Figure A1. Key steps in assessing the operational risks of a payment system using electronic payment instruments