Bank of Russia

GUIDELINES FOR THE ADVANCEMENT OF INFORMATION SECURITY IN THE FINANCIAL SECTOR FOR 2023–2025

Moscow
2023

CONTENTS

The Guidelines for the Advancement of Information Security in the Financial Sector for 2023–2025 were approved by the Bank of Russia Board of Directors on 22 May 2023.

This document was prepared by the Information Security Department.

Cover photo: Shutterstock/FOTODOM
12 Neglinnaya Street, 107016 Moscow
Bank of Russia website: www.cbr.ru

INTRODUCTION

To enhance cyber security and cyber resilience in credit and financial institutions in 2019–2021, the Bank of Russia implemented four key objectives set in the Guidelines for the Advancement of Information Security in the Financial Sector for 2019–2021 (hereinafter, the Guidelines for 2019–2021). The Guidelines for 2019–2021 were approved by Minutes of the Meeting of the Bank of Russia Board of Directors No. 23, dated 6 September 2019.

In the course of the implementation of the Guidelines for 2019–2021, the Bank of Russia achieved the following results:

1. Within the objective 'Cyber security and cyber resilience to enhance the financial stability of each financial market organisation', the Bank of Russia:

- Developed proportionate regulatory requirements for the protection of information in the course of provision of banking services, operations in financial markets, and money transfers in the Bank of Russia Payment System.
- Organised the supervision in the area of cyber security, in particular:
  - Arranged a regular calculation of all credit institutions' and major non-bank financial institutions' risk profiles. Risk profile indicators were included in financial associations' composite risk profile.
  - Organised remote and on-site supervision on a regular basis.
  - Developed the methodology for regular cyber trainings.
- There are no facts of disturbances of financial stability as a result of successful cyber attacks.

2. Within the objective 'Operational reliability and business continuity of credit and financial institutions', the Bank of Russia:

- Developed proportionate regulatory requirements for all supervised credit and financial institutions. With its powers to set the requirements for operational resilience stipulated by law, the Bank of Russia established the requirements for operational resilience for credit and non-bank financial institutions.
- Arranged a regular calculation of all credit institutions' and major non-bank financial institutions' risk profiles related to operational resilience issues.
- Integrated operational resilience issues into the management of operational risk.

Within the implementation of the Guidelines for the Advancement of Information Security in the Financial Sector for 2023–2025 (hereinafter, the Guidelines for 2023–2025), the Bank of Russia will continue supervision over operational resilience and business continuity in credit and finance.

3. Within the objective 'Countering cyber attacks, including with the use of innovative financial technologies', the Bank of Russia:

- Developed proportionate regulatory requirements for information protection and operational resilience to be complied with by new financial market participants (operators of information systems where digital financial assets are issued, digital financial asset exchange operators, financial platform operators, and investment platform operators).
- Implemented the information protection requirements for key infrastructure projects in the financial market, namely the Unified Biometric System, the Faster Payments System, the Bank of Russia Payment System, and the Financial Messaging System.
- Arranged information exchange regarding anti-hacking protection between the Financial Sector Computer Emergency Response Team (FinCERT) of the Bank of Russia's Information Security

Department and all credit and financial institutions supervised by the Bank of Russia. There are over 800 institutions participating in the information exchange. The FinCERT performs the functions of the sectoral centre communicating with the State System for Detecting, Preventing and Eliminating Consequences of Computer Attacks on Information Resources of the Russian Federation (GosSOPKA).

- There are no facts of systemic failures in the financial market that would be caused by successful cyber attacks.

4. Within the objective 'Protection of financial consumers' rights':

- Legal, organisational and technological conditions were created to counteract money transfers not authorised by customers.
- A legal framework was established to extrajudicially limit access to internet resources used to commit fraud in the Russian Federation. The mechanism for blocking websites was developed within the collaboration between the Bank of Russia and the Prosecutor General's Office of the Russian Federation. The time for website blocking was decreased from several weeks to several days.
- The Bank of Russia implemented measures to improve cyber literacy across various categories of people. In particular, the regulator developed information and awareness-raising materials and posted them on transport and in social organisations and carried out trainings for talented children and young people at the educational centre Sirius, as well as a cyber quiz and an online financial test.
- Developed the requirements for cyber security staff training. Specifically, the Bank of Russia estimated the demand for specialists, carried out the practice-oriented training CyberCourse for 7,000 specialists, signed agreements with higher education institutions, and carried out an expert examination of educational programmes to train bachelors, specialists and masters in the area of cyber security in credit and finance.

Within the implementation of the Guidelines for 2023–2025, the regulator will continue its efforts aimed at combating social engineering in the banking sector.

In the course of the implementation of the Guidelines for 2019–2021, the regulator signed 11 agreements (memorandums) on exchanging experience and enhancing security in financial services, participated in the creation of the BRICS Working Group on Security in the Use of ICTs, arranged information exchange with the EAEU and BRICS member states and incident response teams, and ensured the participation of its experts in international organisations' work in the area of cyber security.

Furthermore, the regulator achieved the target indicators stipulated in the Guidelines for 2019–2021:

LEVEL OF CONFIDENCE *Table 1*
(%)

	Target	Actual
2018	60	70.9
2021	60	58.5*

** The indicator calculation method was adjusted. As of the end of 2021, the indicator reached 73.32%.*

UNAUTHORISED FINANCIAL TRANSACTIONS *Table 2*
(%)

	Target	Actual
2018	0.005	0.0023
2021	0.005	0.0013

OPPORTUNITIES AND CHALLENGES FOR THE DEVELOPMENT OF THE RUSSIAN FINANCIAL MARKET

Considering the current trends, it is possible to identify several challenges altering the conventional approaches to ensuring cyber security in credit and finance:

- Operational resilience and information protection in the conditions of a decrease in the risk of credit and financial institutions' and infrastructures' technology dependence on external counterparties.
- Protection of financial consumers' rights within a reduction in the percentage of unauthorised transactions.
- Enhancing confidence in financial services amid the rapid evolution of technologies.

The potential of technologies, including payment and financial ones, is one of the factors promoting the development and helping address emerging challenges.

The Guidelines for the Advancement of Information Security in the Financial Sector for 2023–2025 continue the Guidelines for 2019–2021.

When developing the Guidelines for 2023–2025, the Bank of Russia took into account the following strategic documents:

- Information Security Doctrine of the Russian Federation, approved by Executive Order of the Russian President No. 646, dated 5 December 2016.
- Strategy for the Development of the Information Society in the Russian Federation for 2017–2030, approved by Executive Order of the Russian President No. 203, dated 9 May 2017.
- Economic Security Strategy of the Russian Federation, approved by Executive Order of the Russian President No. 208, dated 13 May 2017.
- National Security Strategy of the Russian Federation, approved by Executive Order of the Russian President No. 400, dated 2 July 2021.
- Basic Principles of the Russian Federation State Policy in the Field of International Information Security, approved by Executive Order of the Russian President No. 213, dated 12 April 2021.
- Strategy for the Improvement of Financial Literacy in the Russian Federation for 2017–2023, approved by Directive of the Government of the Russian Federation No. 2039-r, dated 25 September 2017.
- Russian Financial Market Development Programme for 2023–2025.
- National Payment System Development Strategy for 2021–2023.
- Guidelines for the Development of the Bank of Russia's Data Management System for 2022–2024.
- Priorities of the Financial Inclusion Programme of the Russian Federation for 2022–2024.
- draft Financial Market Digitalisation Guidelines for 2023–2025.
- Action Plan (Roadmap) in SupTech and RegTech at the Bank of Russia Until 2023.

The Guidelines for 2023–2025 set the following key objectives for the enhancement of cyber security in credit and finance:

- Protection of financial consumers' rights and enhancement of confidence in digital technologies.
- Promotion of the conditions for safe implementation of digital and payment technologies and ensuring technological sovereignty.
- Ensuring control of cyber security and operational resilience risks for maintaining the continuity of banking and financial services.

The achievement of the above objectives is inseparable from the balancing of the interests of people, businesses and the government in the course of the implementation of the Guidelines for 2023–2025.

In order to monitor the progress in the achievement of the cyber security objectives, the Bank of Russia developed a set of comprehensive indicators:

Target indicator	2021	2022	2025
Public satisfaction with the security level of financial services provided by credit and financial institutions	58.5%	62.6%	At least 70%
Percentage of cyber security measures, implemented as scheduled, that are needed to deploy digital and payment technologies	–	–	At least 90%
Percentage of systemically important credit institutions and major financial institutions that had no cyber security and operational resilience incidents over the calendar year that could affect the achievement of the target indicators of their operational resilience as regards the continuity of financial services	–	–	At least 95%

The Guidelines for 2023–2025 will be implemented in cooperation with federal executive authorities, credit and financial institutions, experts, and the academic community.

1. PROTECTION OF FINANCIAL CONSUMERS' RIGHTS AND ENHANCING CONFIDENCE IN DIGITAL TECHNOLOGIES

In 2022, the amount of unauthorised transactions increased by 4.29% year-on-year, to reach ₽165.44 million. This growth happened amid the active development of new remote payment and financial platforms and a larger amount (+39% to ₽1,458.6 trillion) of money transfers through electronic means of payment. As banks expanded the range of their anti-fraud measures, the number of unauthorised transactions dropped by 15.31% in 2022, compared to 2021, namely to 876,590.

In 2022, unauthorised transactions accounted for 0.00097% (vs 0.00130% in 2021) in the overall amount of money transfers. These figures are lower than both the target percentage of such transactions in total payment card transactions set by the Bank of Russia (0.005%) and a similar limit of the European Banking Authority (EBA)[1].

According to the analysis, a significant percentage of thefts are committed through social engineering, that is, by manipulating people to obtain their personal and financial data. Such thefts increased by 1% year-on-year to reach 50.4%.

1.1. Combating unauthorised transactions and social engineering

The Bank of Russia plans the following measures to counteract unauthorised transactions:

- **Improvement of funds protection and chargeback mechanisms, specifically:**
  - chargebacks considering the actual values of the target indicators and the effectiveness criteria of credit institutions' anti-fraud procedures;
  - limiting remote access to electronic means of payment;
  - enhancement of the quality of credit institutions' anti-fraud procedures;
  - a reduction in the risks of manipulation of the chargeback procedure by customers;
  - protection against droppers (by promoting the conditions where money thefts become cost-ineffective and unprofitable); and
  - enhancement of the quality of the filling-in of payees' details in unauthorised transactions.
- **Information exchange with the Russian Ministry of Internal Affairs using the regulator's database on actual and attempted unauthorised money transfers.** This measure is aimed at enhancing prompt communication and the exchange of information available to the Bank of Russia and the Russian Ministry of Internal Affairs (MIA), coordinating the efforts to detect money withdrawal schemes, and implementing the mechanism for banks to limit access to accounts if the information on transactions is on the Bank of Russia's and the MIA's databases of unlawful acts.

Additionally, it is planned to explore the issue of improving the quality of information on the Bank of Russia's database (feeds) taking into account the following approaches:

- automation and online processing of requests for the exclusion from the Bank of Russia's database (feeds);
- factoring in the results of credit institutions' assessment of information on the Bank of Russia's database (feeds) when considering requests related to unauthorised transactions;
- advancement of centralised tools for distributing attribution data that are involved in unauthorised transactions (feeds) to the level of tools for analysing business entities' reputation, considering the data available in the operations centre infrastructure of payment system operators; and
- integration of device digital footprints in the set of data on unauthorised transactions (feeds).

- **Enhancement of credit institutions' operational risk assessment tools by adding quality parameters of anti-fraud procedures.** The Bank of Russia plans to expand the requirements for

[1] 0.005% (5 euro cents per 1,000 euros transferred).

operational risk management by adding the control metrics of cyber security risk, including the following metrics characterising the proportion (in terms of number and value) of:

- unauthorised (fraudulent) transactions in the total amount of money transfers;
- transactions where a credit institution erroneously stopped the execution of a customer's transaction order in the total amount of unauthorised (fraudulent) transactions; and
- transactions where a credit institution erroneously failed to stop the execution of a customer's transaction order in the total amount of unauthorised (fraudulent) transactions.

- **Development of legally important channels for applying to law enforcement agencies (Unified Portal of Public and Municipal Services (Functions); remote banking systems).** This measure will help speed up and thus contribute to fraud investigation as the enhancement of criminal investigation procedures is crucial to adequately protect the interests of credit institutions' customers given the wide spread of social engineering.
- **Introduction of personal liability for executives in cases where they breach personal data protection laws.** The measure is aimed at preventing leaks of information containing personal data and/or banking secret. It is planned to legally stipulate qualification and business reputation requirements for credit and financial institutions' executives in charge of cyber security and information protection.
- **Improvement of the security of online lending.** Increasing accessibility of financial services and the transition to remote channels for their provision involve considerable risks of the development of fraudulent practices for the receipt of consumer microloans (loans) by third parties through social engineering techniques. To reduce the said risks, it is planned to implement a procedure entitling individuals to establish (cancel) a ban in their credit histories on conclusion of consumer microloan (loan) agreements with them by submitting a relevant application to any credit institution or qualified credit history bureau.
- **Enhancement of identification and anti-fraud procedures at microfinance organisations** to ensure information protection and combat unlawful actions in the course of provision of microfinance organisations' services.
- **Development of financial institutions' cooperation with communication and telematics operators to counteract social engineering in the exchange of information on customers (subscribers)** in order to reduce the risks of unauthorised transactions through social engineering, including by using communication operators' services.In addition, it is planned to explore possible customer tools for the safe use of communication operators' services, including:
  - number identifiers and voice assistants;
  - tools for categorising communication operator subscribers' communications; and
  - tools notifying customers (prior to a money transfer) of any signs of an unauthorised transaction or a phishing or fraudulent resource.
- **Enhancement of sentiment analysis to assess supervised institutions' risks.** The Bank of Russia plans to develop approaches to estimating sentiment considering the issues of cyber security, operational resilience and counteraction to unauthorised transactions through social engineering, as well as the extent of its impact on credit and financial institutions' activity and financial consumers' behaviour. This information will help identify trends in the financial sector more quickly and forecast financial consumers' behaviour patterns. To this end, the regulator is going to develop and implement processes for collecting, processing and analysing information from multiple sources, specifically mass media, social networks, and publications, including in messengers.

1.2. Combating cyber attacks

Within the objective 'Countering cyber attacks', the Bank of Russia plans to:

- **Develop and enhance information exchange between the Bank of Russia and financial institutions regarding cyber attack tactics and techniques.** In particular, this is needed to develop

cyber training scenarios and respond to cyber attacks more quickly, among other things. To make the response to cyber attacks and cyber attack chains more efficient and increase the quality of cyber incident investigation, the Bank of Russia plans to further develop the information exchange between the FinCERT and credit and financial institutions. To this end, the regulator will improve the forms and procedure for exchanging information on actual and attempted money transfers unauthorised by customers.

The Bank of Russia plans to further upgrade the FinCERT's technical infrastructure used for informing credit and financial institutions in order to implement new approaches to the form of data communication. This will accelerate the interaction and help respond to cyber attacks promptly (including proactively).

Additionally, the regulator plans to develop algorithms for creating the FinCERT's information bulletins and attack scenarios for cyber trainings.

- **Enhance the information exchange between the FinCERT and credit and financial institutions to counteract cyber attacks.** The Bank of Russia plans to further upgrade the technical infrastructure of the FinCERT, performing the functions of the sectoral centre of the GosSOPKA, that is used for informing credit and financial institutions in order to implement new approaches to the form of data communication. This will accelerate the interaction and response to cyber attacks.
- **Ensure that non-bank financial institutions classified as major financial market infrastructures and critical information infrastructure entities implement measures to counter targeted cyber attacks depending on their hazard level.** In order to maintain the continuity of financial services, the Bank of Russia will further develop and update the requirements (within the operational resilience) for non-bank financial institutions classified as critical information infrastructure entities to combat targeted cyber attacks depending on their hazard level specified by the federal executive agency in charge of the security of the critical information infrastructure of the Russian Federation.

1.3. Digital financial literacy

Within the objective 'Improvement of digital financial literacy', the Bank of Russia plans the following measures:

- **Programmes for improving digital financial literacy and promoting cyber hygiene among various groups of the population, including low-income and socially disadvantaged people.** To ensure safety in the course of provision of financial services, the Bank of Russia plans to put a special focus on the development and promotion of the basic skills and mindsets in the area of digital financial literacy and cyber hygiene among socially vulnerable groups of people. To this end, the regulator will organise awareness-raising and educational events using modern teaching technologies and productive differentiated learning formats, as well as a competency-based approach and developmental teaching.

The development of the talent pool, specifically the engagement of the youth and elderly people in awareness-raising and educational efforts, will require the creation of educational content and engagement of volunteers promoting digital financial literacy and cyber hygiene. This will help establish a network of social contacts to promote the basic skills and mindsets in the area of digital financial literacy and cyber hygiene among the target groups of people.

The Bank of Russia plans to develop awareness-raising content for notifying people of fraudulent schemes and fraudsters based on the analysis of data. To do this, the regulator will switch to the systemic use of the advanced analysis of data protection incidents and the results of their investigation.

- **The use of a single competencies framework on financial literacy (hereinafter, the Framework) to improve digital financial literacy and promote cyber hygiene.** The Framework stipulates the core financial literacy competencies for schoolchildren (aged 15 and over) and adults and is the basis for the development of various tools enhancing financial literacy (including digital financial literacy and cyber hygiene), namely educational programmes, extended learning programmes, Olympiads, etc. The Framework describes the general sections and training results on the topics at the basic and advanced levels.

The goal is to help Russians form necessary competencies and skills in digital financial literacy and cyber hygiene that would promote the safe use of financial products and services.

The Framework will be the basis for the development of awareness-raising materials, programmes and courses on digital financial literacy and cyber hygiene.

A priority task is the consolidation and use of the basic and advanced digital financial literacy and cyber hygiene competencies within all awareness-raising and educational initiatives in the following three categories:

- awareness, knowledge and understanding;
- confidence, motivation and mindset; and
- skills and behaviour.

The regulator is going to organise instructional events and practice-oriented trainings for the teaching staff incorporating digital financial literacy and cyber hygiene issues in educational programmes, including to study methods and techniques for countering social engineering in the financial market.

- **Posting social ads and distribution of awareness-raising content and programmes on countering social engineering and improvement of digital financial literacy among people.** Jointly with the Russian Government and the constituent territories of the Russian Federation, the Bank of Russia plans to further develop awareness-raising materials (visual, audio and video content) to be distributed on transport and in social organisations and cover digital financial literacy and cyber hygiene issues in federal, regional and local mass media. When developing the content, the Bank of Russia will factor in social and psychological peculiarities of various categories of people related to the perception of such information.

The Bank of Russia will develop and regularly update the awareness-raising content based on the advanced analysis of data on fraudulent schemes and fraudsters. In addition, it is planned to form an expert community that would create a synergistic effect from the exchange of knowledge and practices in content development and adaptation taking into account people's cognitive abilities and the peculiarities of behaviour and information perception by various categories of Russians.

- **Enhancement of awareness-raising work by financial institutions to make customers preserve their personal and financial data more cautiously.** The regulator plans to expand the use of awareness-raising tools by credit institutions to make their customers be more cautious when conducting financial transactions, including money transfers.

Considering the analysis of financial consumers' behaviour patterns, it is planned to update approaches and, if needed, legally stipulate new approaches to informing financial consumers about possible risks of unauthorised access to personal and financial data and unauthorised transactions through social engineering.

2. PROMOTION OF THE CONDITIONS FOR SAFE IMPLEMENTATION OF DIGITAL AND PAYMENT TECHNOLOGIES AND ENSURING TECHNOLOGICAL SOVEREIGNTY

The rapid development of digital technologies has significantly changed financial consumers' needs and expectations. Customers are becoming more demanding, focusing on their consumer experience that is directly associated with digitalisation and the use of technologies. Customers wish to have the option of remote access to a broad range of services in all areas of their life. They prefer convenient, simple and fast services that do not require repeated authorisation and entry of their personal data.

On the other hand, the rapid evolution of technologies involves considerable risks of cyber attacks on customers and financial institutions, as well as fraud in the financial market.

2.1. Development of the regulation

The Bank of Russia plans to form the conditions for ensuring cyber security and cyber resilience of digital and payment technologies through the regulation and follow-up supervision in the following top-priority areas:

- Digital profile.
- Marketplace.
- Open APIs in the financial market, open banking APIs in the National Payment System, and non-bank payment service providers' APIs.
- Electronic document storage.
- Ecosystems.
- Unified Information System for Subscriber Data Verification.
- Ensuring cyber security for new payment and money transfer initiation methods (smart devices and others).
- Unified Biometric System and commercial biometric systems.
- New entities of the National Payment System (non-bank payment service providers and others).
- Data exchange of these credit and financial institutions with regard to their cyber security, including integrity.
- Environment of confidence in the course of remote provision of financial services and programmes for the implementation of cyber security protocols.

Enhancing further the regulation, the Bank of Russia will implement initiatives for establishing legal mechanisms ensuring cyber security and cyber resilience in digital and payment technologies. In furtherance of the single state policy in the area of cyber security and cyber resilience, these approaches will be agreed upon with the Federal Security Service of Russia and the Federal Service for Technical and Export Control of Russia.

The Bank of Russia is going to expand the range of supervisory tools and practices relying on the principle of proportionality and reasonableness for supervised credit and financial institutions to properly comply with the requirements for information protection and operational resilience.

The Bank of Russia will continue the monitoring of the international agenda on cyber security and cyber resilience in digital and payment technologies, using this process, among other things, to protect the national interests in the course of the development of international approaches to technical and technological processes of ensuring cyber security and cyber resilience, as well as to promote best Russian approaches and practices.

As before, a critical objective is to develop cyber security specialists' practical skills in responding to cyber attacks and investigating cyber incidents related to digital and payment technologies. The practical skills are planned to be developed within the practice-oriented training programme.

2.2. Advancement of the national payment infrastructure and the digital ruble

The Bank of Russia will continue to form the conditions for implementing innovative products and services, while maintaining the environment of confidence among payment industry participants by setting cyber security standards that would ensure the continuity of money transfers, accessibility of payment services, and a reduction in financial market participants' losses caused by fraud, including social engineering.

The top-priority areas are as follows:

- Development of cyber security standards expanding access to the Bank of Russia Payment System, including for non-residents.
- Advancement of the Faster Payments System (FPS), namely:
  - implementation of cyber security mechanisms ensuring the FPS interoperability, including the integration of the Russian FPS with similar systems of the EAEU member states;
  - expansion of access to the FPS, including for non-residents;
  - advancement of the cyber security risk management system; and
  - ensuring cyber security and resilience of the mobile application SBPay.
- Advancement of the Financial Messaging System (FMS) in the following areas:
  - enhancement of the cyber security standards expanding access for non-residents;
  - ensuring cyber security in the course of the implementation of new services in the FMS;
  - development of the service bureau institute with regard to cyber security mechanisms;
  - provision of internet access to the FMS; and
  - support of cyber security standards ISO 20022 in the FMS.

In order to develop cross-border payments in rubles, increase the role of the ruble and promote it beyond the Russian Federation, as well as to support exports of payment services to other countries, the Bank of Russia plans to elaborate the issues of cyber security and cyber resilience for ensuring access to the services of the Bank of Russia Payment System, the FPS and the FMS for EAEU banks and other non-resident organisations.

- The digital ruble:
  - stipulation of the information protection requirements for digital ruble platform participants and support for digital ruble platform participants in the area of cyber security;
  - creation of the legal and organisational framework to develop mechanisms for assessing compliance, control of resilience to immediate threats, and testing of applied technologies, algorithms, hardware and software with regard to cyber security issues; and
  - development of anti-fraud mechanisms (monitoring of transactions to detect anomalies suggesting possible fraudulent actions and compromise of digital ruble platform participants) considering the specifics of digital ruble transactions.

To support the use of the digital financial infrastructure by financial market participants, the Bank of Russia will continue to form the conditions for financial institutions to safely deploy digital and payment technologies within the following projects:

- Development of new identification and authentication methods.
- Development of remote identification for residents and non-residents.
- Development of digital financial assets, utilitarian digital rights, and crowdfunding.
- Expansion of opportunities for using electronic signature in the mass segment.

- Creation of the operator of the automated information system (AIS) of insurance, and support for insurance history bureaus.
- Development of communication between credit and financial institutions and federal executive authorities, including access to state data systems (including the Unified Biometric System (UBS), the Unified System of Identification and Authentication (USIA), and Goskey).

The Bank of Russia will continue to elaborate the requirements for cyber security and cyber resilience of digital and payment technologies considering immediate cyber threats and risks, as well as to monitor the actual level of security and cyber resilience of the projects in progress. The regulator will develop the requirements, methodology and practical tools for ensuring cyber security and cyber resilience of digital and payment technologies jointly with federal executive authorities and credit and financial institutions relying on the principles of reasonable centralisation and maximum automation of data exchange processes.

2.3. Experimental legal regimes and regulatory sandbox

The Bank of Russia will continue to explore innovative financial products, suggested by market participants, for their cyber security and cyber resilience within the regulatory sandbox and to form the approaches to ensuring cyber security and cyber resilience when piloting innovative products, services and technologies in banking and other segments of the financial market.

The Bank of Russia plans to carry out the validation of innovative financial technologies, products and services within its regulatory platform, taking into account the comprehensive analysis of information security risk (cyber risk). A similar approach will be applied to new business models and solutions within experimental legal regimes. In addition, the Bank of Russia plans to develop tools for monitoring cyber security incidents within the said regimes.

Considering the results of examination of financial products in the regulatory sandbox or their piloting within experimental legal regimes, the Bank of Russia will continue to enhance the legal regulation in the area of cyber security and cyber resilience.

2.4. Technological sovereignty

To reduce the risk of financial institutions' and infrastructures' technology dependence on external suppliers, the Bank of Russia will coordinate the operations of credit and financial institutions. To this end, the Bank of Russia has established the industry centre of expertise (testing) for the financial sector of the economy that will control the risks associated with the use of foreign information technologies and ensure their import substitution considering the following approaches:

- setting priorities in import substitution with regard to the range of software and hardware;
- implementation of the mechanism for assessing the maturity of solutions from Russian manufacturers and information technology providers;
- selection of options for treating the risks of using foreign information technologies;
- distribution of technical testing tasks across credit and financial institutions, as well as consolidation and disclosure of the obtained testing results;
- communication with competent federal executive authorities, Russian manufacturers and information technology providers;
- experience exchange in this area, including with organisations from other industries;
- preparation of a consolidated request from the credit and financial sector to competent federal executive authorities for the purchase or development of domestic information technologies for the benefit of credit and financial institutions, specifically to form targeted funding for market leaders in certain technological sovereignty areas meeting the needs of the credit and financial sector to the fullest extent possible;

- distribution and ensuring the performance of technical functions of the testing of IT solutions with the use of credit and financial institutions' resources; and
- exercising control over the progress of import substitution within the Bank of Russia's effective powers in ensuring operational resilience.

A critical task related to technological sovereignty will be to ensure cyber security, including by using Russian cryptographic tools in important payment systems. To this end, the Bank of Russia plans to:

- organise the testing by credit institutions of Russian hardware security modules to be used in payment card systems; and
- amend the rules of payment systems for the implementation of the requirements stipulated by Bank of Russia Regulation No. 719-P, dated 4 June 2020, 'On the Requirements for the Protection of Information Related to Funds Transfers and on the Procedures for the Bank of Russia to Control Compliance with the Requirements for the Protection of Information Related to Funds Transfers'.

The Bank of Russia plans to take part in the development by federal executive authorities of the cyber security requirements for critical information infrastructure entities–credit and financial institutions.

3. ENSURING CONTROL OF CYBER SECURITY AND OPERATIONAL RESILIENCE RISKS FOR MAINTAINING THE CONTINUITY OF BANKING AND FINANCIAL SERVICES

Creating the conditions for the safe provision of financial services, including with the use of innovative digital and payment technologies, the Bank of Russia takes into account general trends in supervision over both the financial sector and the information technology and cyber security industry. The Bank of Russia's objectives are to ensure the continuity of banking and financial services (operational resilience) and control cyber security risks for early detection of risks that might affect credit and financial institutions' financial stability.

3.1. RegTech and SupTech projects

In order to develop RegTech and SupTech projects, the Bank of Russia plans to:

- **Enhance external cyber security audit.** The task of ensuring the quality of assessment of information protection in credit and financial institutions was set as part of the initiative provided for by the SupTech and RegTech Development Guidelines for 2021–2023.

In the course of the elaboration of the concept for enhancing the system of external cyber security audit, the Bank of Russia is going to explore the issue of creating additional legal mechanisms for improving the quality of assessment of information protection in credit and financial institutions and the quality of audit companies' services. These mechanisms will be used to develop the requirements for ensuring the reliability of external audit results by engaging audit companies checked for conformity of their operations with the national standards that are identical to international ones.

The external audit system is planned to be implemented in the following areas:

- audit of cyber security and operational resilience issues;
- audit of cloud providers; and
- audit of the security of applications.

- **Implement the system of monitoring and analysis of credit institutions' operational risks.** The Bank of Russia plans a complex of measures for monitoring and analysis of cyber security risks being part of operational risks in accordance with Bank of Russia Regulation No. 716-P, dated 8 April 2020, 'On the Requirements for the Operational Risk Management System in a Credit Institution or a Banking Group'.

An important area will be the fundamental transition to the systemic use of the advanced analysis of credit institutions' operational risks considering the data formed as a result of:

- analysis of cyber security and operational resilience incidents;
- calculations of credit and financial institutions' and financial associations' risk profiles;
- supervision, including in the form of cyber trainings; and
- analysis of the data from reporting forms on operational risk management and ensuring operational resilience.

The Bank of Russia plans to integrate the results of monitoring and analysis of credit institutions' operational risks into the assessment of credit institutions' economic situation, financial stability recovery plans and the quality of internal capital adequacy assessment processes (ICCAP) with regard to:

- cyber security risk;
- cyber security risk associated with possible unauthorised transactions; and
- cyber security risk associated with a possible disruption of operational resilience.

Additionally, the Bank of Russia will explore the issues of the development, testing and further adjustment of the methods for assessing supervised credit and financial institutions' opportunities to detect cyber security and operational resilience incidents, respond to them and recover in the case of their occurrence, as well as the methods for assessing the organisation of the cyber security and operational resilience risk management system.

- **Create a legal framework for information technology outsourcing and using cloud systems by financial institutions** (for details, see Section 3.4).

3.2. Cyber trainings

The Bank of Russia plans to continue the development of the supervisory stress testing of credit and financial institutions to ensure cyber security and operational resilience within the expansion of the range of scenarios, issues and tasks considered in the course of cyber trainings.

The measures to be implemented in this area will help ensure control of credit and financial institutions' operational risks in the said areas in the conditions of the transition to technological sovereignty, as well as control over the quality of IT services provided to customers and counterparties.

Within cyber trainings, the Bank of Russia plans to carry out:

- Cyber trainings (stress testing) at credit and financial institutions.
- Cyber risk assessment for the integration into the supervisory assessment of operational risk with regard to:
  - cyber security risk;
  - cyber security risk associated with possible unauthorised transactions; and
  - cyber security risk associated with a possible disruption of operational resilience.

The Bank of Russia plans to develop a scenario approach within the supervisory stress testing for assessing supervised credit and financial institutions' resilience to cyber security and operational reliability incidents.

The results of the cyber trainings will be used in the system of monitoring and analysis of credit and financial institutions' operational risks.

3.3. Risk profiling

The Bank of Russia will continue the practice of risk profiling of supervised institutions to assess actual cyber security and operational resilience risks. Risk profile parameters are used within the implementation of the general process for organising and carrying out cyber trainings in the course of supervisory measures and are taken into account when selecting a supervisory regime for credit and financial institutions. To this end, the Bank of Russia plans to:

- Develop cyber risk measures, including measures of outsourced service providers' risks, with regard to cyber security and operational resilience risks, namely:
  - cyber security risk;
  - cyber security risk associated with possible unauthorised transactions; and
  - cyber security risk associated with a possible disruption of operational resilience.
- Develop the mechanism for the cyber risk profiling of financial institutions.
- Monitor and detect cyber risks affecting financial stability and operational resilience of major financial institutions, financial associations and financial ecosystems.

The results of the risk profiling will be used in the system of monitoring and analysis of credit and financial institutions' operational risks.

3.4. Information technology outsourcing and using cloud systems

Using the services of information technology and cloud outsourcing providers, credit and financial institutions need to pay particular attention to the outsourced business processes and functions subject to the Bank of Russia's information protection and operational resilience regulation. Besides, information technology and cloud outsourcing providers shall fully comply with the laws regulating the performance of outsourced business processes and functions. This approach is in line with the international practice.

Within this objective, the Bank of Russia plans to:

- Enhance the institute of information technology and cloud outsourcing for financial institutions taking into account cyber risks.
- Monitor the risks of information technology and cloud outsourcing.
- Develop the mechanisms for using cloud systems in credit and finance. In order to enhance the institute of outsourcing of information technologies and cloud services of information systems and their components, namely cloud and file storages, servers and other data collection, storage and processing devices and systems, the Bank of Russia plans to create, jointly with competent federal executive authorities, a legal framework for hosting, storage and other processing of the data obtained within credit and financial institutions' operations. Besides, the concept provides for the use of outsourcing service providers' information systems and their components and for the stipulation of the legal status of an information technology and cloud outsourcing provider that shall then comply with the requirements for ensuring the protection of banking secret and other types of secrets protected by law.

In furtherance of the standards forming the conditions for the use of outsourcing services, the Bank of Russia plans to establish the procedure for communication in the course of information technology and cloud outsourcing and to develop the requirements for risk management in the course of outsourcing.

To ensure full compliance with the information protection and operational resilience requirements, the Bank of Russia will continue to enhance the range of its supervisory tools and practices for the analysis of risks associated with the use of outsourcing services, including to develop the tools for determining the threshold concentration of outsourcing service providers that suggests the existence of systemic risks.

Basic block. International cooperation

The Bank of Russia will continue the development of international cooperation in cyber security provided for by the Guidelines for 2019–2021. This will ensure the continuity of the approaches to the development at the global, regional, multilateral and bilateral levels of cooperation of the Russian Federation in the area of cyber security and operational resilience, as well as its competent participation in the development of an up-to-date agenda meeting Russia's interests.

As before, the main objectives in the current conditions are the development of experience exchange with central (national) banks in the regulation and implementation of financial technologies.

Besides, considering the results of the international cooperation achieved in 2019–2021, the Bank of Russia plans to continue to enlarge the agenda of cooperation and the number of counterparts, on the one hand, and to strengthen and expand the already existing relations through closer and deeper cooperation, on the other hand.

- **Multilateral cooperation.** The Bank of Russia will participate in the activities of international organisations related to the issues of cyber security and cyber resilience by exploring approaches to and best practices of the regulation of and supervision over cyber resilience. This work will be mostly carried out within the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the International Telecommunication Union (ITU).

Among other things, this work will comprise monitoring of the activities of the International Organization of Securities Commissions (IOSCO), the Financial Stability Board (FSB), the Committee on Payments and Market Infrastructures (CPMI), the International Association of Insurance Supervisors (IAIS), and the Basel Committee on Banking Supervision (BIS).

- **Integration cooperation.** Cooperation with the EAEU and BRICS national (central) banks on the exchange of information and best practices in the area of protection of financial consumers' rights and the enhancement of confidence in digital technologies, cyber security and cyber resilience of digital and payment technologies, including the issues of standardisation in the area of cyber security.

- **Bilateral cooperation.** Cooperation with foreign regulators and supervisory authorities on the exchange of information and best practices in the area of cyber security and cyber resilience.

Basic block. Training of cyber security personnel

Frequent problems in both cyber security and IT are a deficit and inadequate competencies of employees. Due to its specifics, cyber security is crucial for the implementation of innovations and new digital and payment technologies. Therefore, the development of the talent pool is a top priority.

- **Introduction of the professional standard Information Security Specialist for Credit and Financial Institutions.** The professional standard as an instrument of the national qualification system was developed jointly with the expert, academic and business communities for the benefit of the credit and financial sector in order to create necessary competencies.

The professional standard stipulates the requirements for work operations, knowledge and skills of cyber security specialists of various levels providing for progressive development and improvement of professional competencies.

In order to enhance the organisational measures for ensuring credit and financial institutions' cyber security and operational resilience, the Bank of Russia plans to update the professional standard on a regular basis, taking into account current challenges and threats.

- **Elaboration of the state higher education standards for training information security specialists in credit and finance.** The professional standards form the basis for the development of education standards. Therefore, the Bank of Russia will explore the issues of the development of the requirements for education and the areas of training for information security specialists in credit and finance. To this end, the Bank of Russia will elaborate approaches to enhancing the federal standards in the areas of training for information security specialists and to developing methodological recommendations on training for information security specialists of various education levels in credit and finance. They will be the basis for the development of training programmes for Russian educational institutions.
- **Implementation of education programmes, including advanced professional education programmes, in cyber security at the leading universities.** In order to apply uniform standards for the quality of training of information security specialists having the fundamental knowledge of the peculiarities of the functioning of the financial market, it is planned to create an innovative education ecosystem for training practice-oriented cyber security specialists in credit and finance, including by combining the fundamental scientific background and high expertise of specialists in the real economy.

The Bank of Russia will continue to create the conditions for training information security specialists of a new type. In particular, it is planned to establish a geographically distributed network of universities implementing education programmes on cyber security in credit and finance.

In addition, the regulator plans to design and create unique educational products on cyber security for talented young people based on the leading scientific and educational centres, consortia and associations of universities of the Russian Federation, as well as the specialised department of the Bank of Russia at the Higher School of Economics.

- **Analysis and planning of the need for information security specialists in credit and finance.**

In order to plan the overall need for cyber security personnel, the Bank of Russia will continue the practice of monitoring of credit and financial institutions' future need for employees. The analysis of the results of the study will help form a model for forecasting the required number of graduates in cyber security and become the basis for the development of educational programmes and products.

- **Improvement of practical skills of information security specialists in credit and finance.** The implementation of a practice-oriented approach to training on cyber security in credit and finance at all levels of the Russian education system will help future specialists form a pool of practical skills.

It is planned to create the conditions for their development in the course of the scientific and research activity of educational institutions focusing on practical aspects and topical issues of cyber security in credit and finance.

The Bank of Russia will implement its educational initiatives, aimed at increasing relevant technical expertise among information security specialists in credit and finance, within practical and project activities.

- **Practice-oriented cyber security training CyberCourse.** To develop information security specialists' practical skills, the Bank of Russia will continue to implement the practice-oriented cyber security training programme CyberCourse. The programme will help update the already existing knowledge base, maintain professional competencies in cyber security, develop interagency cooperation, and decrease the level of cyber crime and cyber fraud in the credit and financial sector as a whole.
- **Regular advanced trainings for academic staff in the area of modern digital financial instruments and technologies.** For students to gain relevant knowledge and competencies in the area of the financial market, the Bank of Russia plans to implement a comprehensive approach to the system of advanced training for academic staff in the area of modern digital financial instruments and technologies. Advanced training will be based on the best practices of credit and financial institutions. It is planned to create an academic community of professionals focusing on the development of teaching practices and methods to provide relevant knowledge in the area of digital financial literacy and cyber hygiene.

Basic block. Dealing with data

- **Data quality and confidence in data.** Implementing the Guidelines for the Development of the Bank of Russia's Data Management System for 2022–2024, the regulator plans to form a systemic approach to ensuring the quality of and confidence in both the data used by the Bank of Russia for making management decisions and the data provided to and received from supervised institutions and participants in the information exchange with the FinCERT.

Within this objective, the Bank of Russia plans to enhance the efficiency of using the types of data needed to:

- calculate supervised institutions' risk profiles;
- carry out advanced analysis of computer attacks; and
- ensure the quality and prompt submission of information about unauthorised transactions.

The automation of data quality management will help ensure real-time monitoring of the data status and analysis for the implementation of the Bank of Russia's strategic objectives of enhancing cyber security in credit and finance.

- **Data and service provision to external users for cyber risk insurance.** International experts estimate the global cyber risk insurance market at $14 billion as of 2022 and as much as $20 billion by 2025. Cyber risk insurance is needed to cover losses caused by successful cyber attacks. The Bank of Russia plans to create the conditions for establishing the institute of cyber risk insurance and provide an expanded list of data to external users to form insurance models.
- **Implementation of data management practices.** The Bank of Russia will develop data management practices to ensure cyber security at supervised institutions and the Bank of Russia, as well as the quality of the data used in risk profiling and the analysis of computer attacks and information on unauthorised transactions.
- **Development of the rules for dealing with data at the Bank of Russia's structural units to ensure cyber security.** In order to implement cyber security management practices, it is planned to develop the rules for dealing with data at the Bank of Russia's structural units, including to determine access objects, uniform rules for data access management, a role-based model of liability, and mechanisms for providing access to datasets.