CENTRAL BANK
OF THE REPUBLIC OF AZERBAIJAN

CYBERSECURITY STRATEGY IN FINANCIAL MARKETS

2023
2026

Contents

1. Executive summary 1
2. Current cybersecurity situation in the financial system of the country 2
2.1. Financial institutions assessment framework 2
2.2. Cybersecurity landscape of financial institutions 3
2.3. Information security and cybersecurity at the Central Bank 4
3. Global cybersecurity trends and main challenges in the financial system 7
4. Best practices from benchmark countries 9
4.1. Australia 10
4.2. United States 11
4.3. European Union 11
4.4. Japan 12
4.5. Singapore 13
5. Cybersecurity strategy in financial markets 14
5.1. Strategic priority 1: Strengthen regulatory and supervisory framework on information security and cybersecurity in financial markets 15
5.2. Strategic priority 2: Strengthening culture of cyber risk management in financial markets 21
5.3. Strategic priority 3: Formulating information technologies governance framework to strengthen the level of cybersecurity in financial markets 22
5.4. Strategic priority 4: Strengthening cyber resilience in financial markets 24
5.5. Strategic priority 5: Formulating information security and cybersecurity culture in financial markets 26
6. Expected outcome 27
7. Actions Plan on cybersecurity strategy in financial markets 29
8. Time table on implementation of the cybersecurity strategy in financial markets 32

1. Executive summary

The current trend of digital financial services, which rely on innovative solutions, not only enhances the effectiveness and efficiency of various activities, but also exposes the financial ecosystem to heightened vulnerability towards cyberattacks. Accordingly, global financial systems have become key targets of cybercriminals, resulting in higher frequency of cyber-attacks and more sophisticated attack scenarios. Related cyber trends, in their turn, necessitate proper cyber risk management and an adequate regulatory framework. Hence, supervisory authorities improve cyber resilience in financial markets continuously and make related actions a part of every initiative.

The main goal of the 'Cybersecurity strategy in financial markets' (Strategy) for 2023-2026 is to strengthen information security and cybersecurity at the Central Bank of the Republic of Azerbaijan (CBA) and financial institutions (FIs) operating throughout the country and determine main activity directions on more effective prevention of cybersecurity threats and cyberattacks of nowadays. Initiatives and would-be actions included to the Strategy are oriented towards elevating the level of preparation of the CBA and financial markets as a whole to possible cybersecurity incidents and emergencies and more effective decision-making arrangements related to cybersecurity initiatives by timely informing stakeholders.

The vision of the Strategy is to **'strengthen cyber resilience in financial markets against evolving cyber threats to safeguard financial stability'**. As a part of the public policy of information security and cybersecurity in the country, this Strategy determines main goals, principles, directions and priority objectives of related activities. The main mission of the Strategy is **to develop financial system, encompassing a robost security infrastructure in the realm of cybersecurity, developing human capital with advanced knowledge and skills, fostering effective cooperation to facilitate the exchange of information on cyber threats, and establishing adequate regulatory framework to ensure cyber resilience of the financial system.**

When formulating the Strategy, the current cybersecurity stance in the financial sector was assessed in accordance with the self-assessment framework developed as part of cooperation with the International Finance Corporation based upon relevant standards of the National Institute of Standards and Technology (NIST) and cybersecurity strategies and approaches applied in benchmark countries were analyzed.

Main targets of the Strategy are to: **1)** formulate a cybersecurity ecosystem in financial markets of the country, adequately respond to cyber threats and elevate cybersecurity level; **2)** boost financial system resilience by prioritizing continuous information sharing as part of cyber hygiene and mutual partnership; **3)** formulate and update continuously normative-methodological basis related to information security and cybersecurity, thus safeguarding financial stability in financial markets of the country within the mandate of the CBA.

2. Current cybersecurity situation in the financial system of the country

International cybersecurity ratings of our country have been improving over recent years because of concerted measures by related public authorities and associations to reinforce and develop the national cybersecurity ecosystem in light of international trends. According to the National Cyber Security Index for 2023, Azerbaijan advanced 33 places in the ranking, ahead of countries, such as Kazakhstan, Belarus, Uzbekistan, and Armenia, and ranked 53rd[1]. Maintaining this growth rate and safeguarding cyber resilience of the financial system, a part of the national cybersecurity ecosystem of our country, has become one of critical priorities. The implementation of this priority necessitates the assessment of the current cybersecurity stance in the financial system.

This section of the Strategy comments upon the self-assessment methodology applied, followed by findings of cybersecurity surveys conducted among various FIs.

2.1. Financial institutions assessment framework

Surveys were conducted in FIs to assess the current cybersecurity stance in financial markets. The surveys covered 51 respondents – FIs, including banks, insurance companies and other financial market participants:

- Banks: 22
- NBCIs: 15
- Insurance companies: 10
- Card processing centers: 2
- Other (the National Depository Center, the Compulsory Insurance Bureau): 2

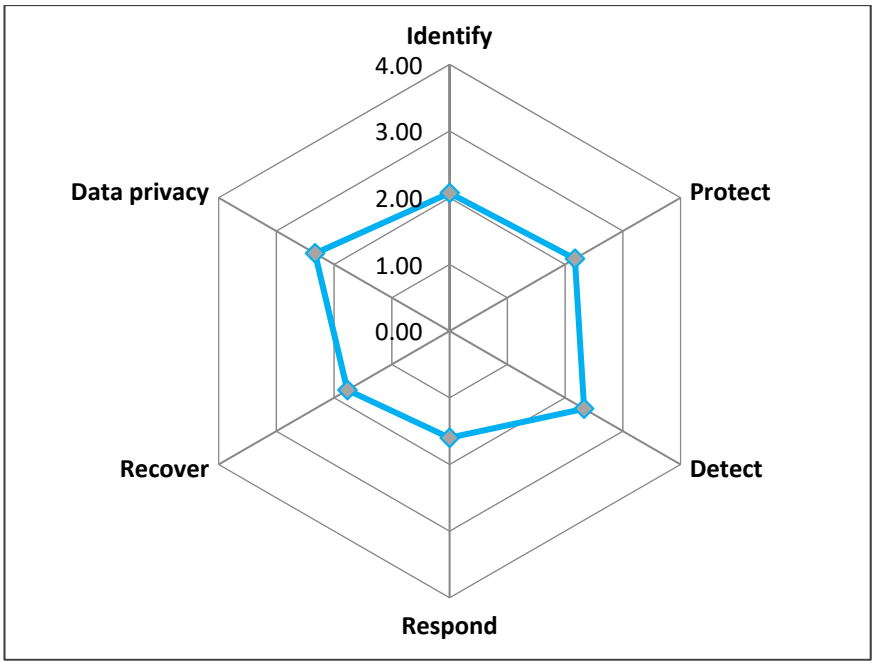
[1] https://ncsi.ega.ee/ncsi-index/?order=rank

The surveys were based upon the cybersecurity framework of the NIST standard and divided into 6 categories and 52 questions. Surveys allowed analyzing the identification and protection of information assets at financial institutions, detection of, adequate response to and elimination of security incidents, as well as data privacy.

2.2. Cybersecurity landscape of financial institutions

Surveys in FIs found out that, indicators on 'response to cybersecurity incidents' and 'recovery of activities' fall below the average cybersecurity indicator of the financial sector (Table 1). To that end, one of the key targets of the Strategy is to increase these indicators by stepwise applying best practices.

Figure 1: Cybersecurity situation in financial markets of the country



Source: Cybersecurity survey findings

As seen from Table 1, the cybersecurity stance is more favorable for the banking sector and payment market participants than for insurance companies involved in the survey. According to the 'Detect security events' indicator, the cybersecurity maturity level of the banking sector and payment system participants is over 2.4. Whereas the average cybersecurity indicator of the financial sector stands at 2.28 for all three segments, the average indicator was 2.14 on the banking sector, 1.85 on insurance companies and 2.85 on payment markets. Hence, participants across all three segments of financial markets should intensify measures to boost cybersecurity and attach great importance to this field.

Table 1: Cybersecurity stance comparison by FIs [2]

Indicators	Banking sector	Insurance sector	Payments market	Average
Identify information assets	2.15	1.9	2.85	**2.3**
Protect information assets	2.2	2.1	3.25	**2.51**
Detect security events	2.4	2.2	3.35	**2.65**
Respond to security events	1.8	1.2	3.15	**2.05**
Recover from security events	1.9	1.5	2.1	**1.83**
Data privacy[3]	2.4	2.2	2.4	**2.33**
Average	**2.14**	**1.85**	**2.85**	**2.28**

Source: Cybersecurity survey findings

2.3. Information security and cybersecurity at the Central Bank

The CBA regulates and supervises financial market participants according to Article 48 of the 'Law on the Central Bank of the Republic of Azerbaijan'. To that end, the CBA conducts comprehensive and thematic inspections at supervised entities and focuses on the assessment of their information security, including protection of individual data. Thus, according to Decision No 161 of the Cabinet of Ministers of the Republic of Azerbaijan dated 6 September 2010 the financial markets supervisory authority is entitled to control the implementation of requirements on personal information protection in financial markets.

Information security and cybersecurity in financial markets entails the formulation of an appropriate legal regulatory framework, including authorities of the CBA on the above area and determining regulatory requirements for financial market participants. Hence, according to the current legislation, including Article 38.3 of the Law of the Republic of Azerbaijan 'on Banks', the CBA determines minimum requirements for banks' maintaining reliability and security of automated settlement and money transfer systems and protection of information they use. To that end, the Bank formulated and continuously updated the normative-legal framework, including minimum information security requirements in relevant periods.

[2] *'Banks' include banks and NBCIs, 'Insurance' includes the CIB and insurance companies, 'Payments market' includes card processing centers.*
[3] *Included as an addendum to the NIST framework*

The ‘Regulation on information security management in banks’ approved by Decision No 20/1 of the Management Board of the CBA dated 14 July 2021 took effect on 1 April 2022[4]. According to the requirements of the ISO/IEC the Regulation includes the formation and organization of the ‘Information security management system’ in banks, safety and security of human resources, asset management, access control, cryptography, physical security and security along the perimeter, protection of information sharing, ensuring security during obtaining, introduction and maintenance of information systems, protection of information security in relations with external suppliers, oversight mechanisms and requirements on management of information security incidents.

The CBA takes overwhelming measures to ensure safe, reliable and uninterrupted activities of payment and information systems supporting mandates and functions of the CBA stipulated with the legislation along with strengthening information security and cybersecurity in financial markets. These measures include activities on the formation of ‘Information security management system’ within the institution, as well as the launch and modernization of critical technological infrastructure. In particular the CBA:

- adopted and continuously updates policies, procedures and activities in the ‘Information security management system’;
- ensured that information security policy covers relevant information risks and areas of control;
- defined information security related obligations and duties on the following objectives:
  - employees and counterparties comply with their information security responsibilities prior to starting operations;
  - measures are taken to ensure information security when working remotely and using mobile devices;
  - awareness processes are in place related to information security and obligations with regards to information security.

[4] https://e-qanun.az/framework/48025

- takes measures to prevent unauthorized disclosure, change, destruction or damage of the information stored in information systems;
- takes measures to restrict access to information and data;
- takes measures to restrict unauthorized access to information systems and software;
- takes measures to ensure correct selection and use of cryptography to protect confidentiality and integrity of information;
- ensures physical security and security on the perimeter within and around the institution;
- takes measures for proper and safe operation of information processing facilities, in particular:
  - application of change management procedures;
  - implementation of malware and code protection;
  - security processes are set with regards to external storage devices;
  - fulfilment of backup and recovery of copies of information systems;
  - perform registration of events and incidents in information systems and process management;
  - identify and prevent vulnerabilities in information systems, etc.
- manages and monitors network infrastructure to maintain information security and cybersecurity;
- ensures security of information transmission inside the institution;
- made sure that information security and cybersecurity is an integral part of information systems over their entire period of use;
- takes the following measures to ensure ongoing and effective management of information security incidents, including communication of security incidents and vulnerabilities:

- ensures continuity of information security in the event of damage, destruction or cyber threat to information systems;
- implements data loss prevention and applies security controls;
- performs procedures to detect vulnerabilities in information systems;
- fulfils procedures on consistent configuration management in information systems;
- ensures incident response activities are effectively coordinated with internal and external stakeholders;
- conducts information security awareness measures;
- provides activities for cyber security readiness and cyber exercises.

3. Global cybersecurity trends and main challenges in the financial system

Global financial systems have become main targets of cyber criminals recently, due to the growing frequency of cyber-attacks, application scenarios are more sophisticated and more costly for those exposed to attacks. Investigations suggest that, the average cost of a data breach in the United States amounted to 9.44 million U.S. dollars in 2022 due to cyber-attacks[5]. FIs are applying new generation security solutions allowing to detect and respond to cyber threats in a real time to fight these threats. The most common cyber-attack trends in the financial system are shown below:

One of the most widespread types of cyberattacks in the financial sector is phishing. As a rule, phishing attacks involve the use of fake e-mails or web pages by obtaining sensitive information like user logins or personal information. FIs accounted for the highest share (27.6%) of total registered phishing attacks in Q2 2022[6]. Cybercriminals can convince people to provide personal and financial information using social engineering techniques. To fight these threats FIs take active communication measures, apply multi-factor authentication and other technical control tools to recognize (distinguish) phishing attacks.

[5] *IBM Cost of a Data Breach Report (https://www.ibm.com/security/data-breach)*
[6] *Phishing Activity Trends Report, 2Q 2022 (https://apwg.org/trendsreports/)*

Ransomware (ransom) is another increasing threat for the financial sector. According to the PwC, ransomware was the most prominent cybersecurity threat faced by most organizations in 2021[7]. 55% of financial system participants was targeted on the same year, data leaks doubled due to ransomware cyberattacks on financial services[8]. To be protected from ransom attacks, organizations should provide a number of security measures, which mainly include awareness events on social engineering cyber-attacks, introduction of multi-factor authentication solutions and procedures on regular creation of backup copies of data.

Insider cyber threats are also of serious concern. Insider cyber threats are maintained by getting privileged access by staff or counterparties of the organization to steal sensitive data or disrupt conduct of operations. Although it is possible to prevent external cyber threats or detect by means of technical tools in the first instance, in most cases those tools are not sufficient to prevent insider threats. To that end, to be protected from insider threats advanced policies and procedures, up-to-date security and technology solutions, and continuous information and awareness measures must be implemented.

Another threat faced by the financial sector is the Distributed Denial-of-Service Attack (DDoS). DDoS attacks load network traffic channels of the targeted information system and make them unavailable. Thus, DdoS attacks in the financial sector doubled in 2021 as in previous years[9]. Consequently, to prevent relevant cyber-attacks, organizations preventive measures, such as filtering in their networks, applying appropriate traffic limits, forwarding data transmitted in network systems through distributed channels, adjusting requests to the network according to their source addresses, and others.

Recently major central banks amplified supervisory measures on management of IT and information security risks and attach great importance to this area. Supervisory units of central banks regular examine the cybersecurity risk management. These inspections should allow detecting cybersecurity and risking management related gaps along with

[7] *Cyber threats 2021: a year in retrospect (https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf)*

[8] *Global threat report (https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2022GTR.pdf)*

[9] *Cyber threats and trends (https://www.cdn.neustar/resources/whitepapers/security/neustar-cyber-threats-trends-2020-report.pdf)*

thematic analyses and continuous supervision. To that end, FIs target the following when regulating information security and cybersecurity risks:

- Align the IT strategy with the overall business strategy;
- Treat IT, information security and cybersecurity risks as part of organizational risk management, form a comprehensive risk register, and apply mechanisms to identify, monitor and eliminate relevant risks;
- Involve staff to adequate cybersecurity risk training and awareness events;
- Formulate and apply relevant data classification related policies and procedures;
- Restrict unauthorized access, including applyication of access management mechanisms and procedures;
- Effectively manage the process of involving external service providers (counterparties), and implement the continuous supervisory mechanisms on information security prior to and after the formation of those service relations;
- Cover all technology based solutions with adequate supervisory mechanisms on information security and cybersecurity;
- Ensure adequacy of disaster recovery and business continuity plans in emergencies and test them under various scenarios continuously.

4. Best practices from benchmark countries

Best practices of the countries like Australia, the USA, the European Union (EU), Japan and Singapore on cybersecurity were analyzed. The cybersecurity ecosystem of the above countries were compared on four key different dimensions: (i) cybersecurity policy and strategy; (ii) regulatory frameworks; (iii) cybersecurity culture; and (iv) cybersecurity education, training and skills.

4.1. Australia

Cybersecurity policy and strategy	The Australian Regulator (APRA) developed a Cybersecurity Strategy 2020-2024. The priority areas in the Strategy are the following: ▪ Establishing a baseline of cyber controls, embedded non-negotiable cyber practices, facilitate better sharing of cyber information and enable more effective cyber incident responses; ▪ Enabling boards and executives of financial institutions to oversee and direct corrections of cyber exposure; ▪ Rectifying weak links within the broader financial ecosystem by advocating cyber-assessment and harmonizing regulation and supervision of cyber across the financial system.
Regulatory frameworks	APRA issued mandatory Prudential Standards in 2019, which aim to ensure that APRA-regulated entities meet certain cybersecurity requirements to be resilient against emerging cyber threats. APRA-regulated entities must: ▪ Define information security-related roles and responsibilities of the management in the organization; ▪ Maintain information security capability commensurate to the size and extent of threats to IT assets; ▪ Implement controls to protect IT assets; ▪ Notify APRA of security incidents.
Cybersecurity culture	Annual Cyber Threat Report: ▪ Largest proportion of cyber incidents are 'moderate' (36.5%) and 'substantial' (33.3%); ▪ Most common types of cyber incidents are grouped as 'malicious e-mails' (27%) and 'compromised systems' (24.4%).
Cybersecurity education, training and skills	Australia will invest AUD 1.6 billion in 10 years to: ▪ Increase the number of certified cyber security professionals; ▪ Increase collaboration to build Australia's cyber skills pipeline; ▪ Advise to small and medium institutions to increase their cyber resilience; ▪ Improve ecosystem awareness of cyber threats.

4.2. United States

Cybersecurity policy and strategy	Different US Administrations have released Cybersecurity Strategies and Cybersecurity Implementation Plans aiming to strengthen the cybersecurity level and identifying strategic priorities.
Regulatory frameworks	The US Federal Reserve require different FIs to adhere to NIST, ISACA and COBIT (card processing centers also PCI-DSS) standards and methodological frameworks.
Cybersecurity culture	According to the 'Pew Research Center': ▪ The population generally fail to follow cybersecurity best practices; ▪ 64% of surveyed suffered a major data breach.
Cybersecurity education, training and skills	▪ NIST maintains cybersecurity events and publications continuously; ▪ National Initiative for Cybersecurity Education (NICE) is a partnership between government and academia, the private sector to address cybersecurity needs related to public awareness, education and professional development; ▪ The National Initiative for Cybersecurity Careers and Studies is an online resource portal for cybersecurity education, training and career opportunities.

4.3. European Union

Cybersecurity policy and strategy	Euro system cyber resilience strategy for FMIs is based on CPMI-IOSCO Cyber Guidance. The strategy is composed of 3 pillars: ▪ FIs cyber resilience: the European Central Bank issued the Cyber Resilience Oversight Expectations (CROE) defining the three levels of an FMI's cyber maturity: (i) Evolving level where all payment systems must meet the Evolving expectations, aspiring to move to Advancing level; (ii) Advancing level which is evolving maturity level plus all SIPS must meet the Advancing expectations, aspiring to move to Innovating level; (iii) Innovating level which is Evolving level plus Advancing maturity level plus Ultimate level. In parallel, the ECB launched the TIBER-EU: EU Threat Intelligence Based Ethical Red teaming, defining ethical hacking/red teaming and making recommendations how to do it with specific Guidelines how to hire ethical hackers. ▪ Sector resilience: through UNITAS, a market-wide exercise scenario and communication procedure have been formulated.
Regulatory frameworks	The initiatives developed by the Joint Committee of the European Supervisory Authorities (EBA, ESMA and EIOPA) on strengthening EU cyber and information security regulation in the financial sector include:

	▪ Developing oversight framework for third party providers active in financial services focusing on cloud services; ▪ Developing a relevant framework for testing cyber resilience of systemically important FIs.
Cybersecurity culture	The 2020 EU Cybercrime survey revealed the following: ▪ 52% respondents affirmed are well informed about cybercrime; ▪ 59% state that they can protect themselves sufficiently against cybercrime; ▪ 10% say that cyber concerns make them less likely to make purchase online.
Cybersecurity education, training and skills	The European Union Agency for Cybersecurity (ENISA) supports many initiatives on cybersecurity awareness: ▪ Guidance for improving Cyber security; ▪ European Cyber Security month; ▪ European Cyber Security Challenge; ▪ Develop mechanisms for cyber incidents and crisis management.

4.4. Japan

Cybersecurity policy and strategy	The Financial Services Agency (FSA) issued the "Policy Approaches to Strengthen Cybersecurity in the Financial Sector" in 2018 to address the digitization. Later, in 2020 the FSA published the "Financial Services Cybersecurity Report" describing common challenges of FIs. The FSA encourages small and medium FIs to maintain and improve effectiveness of their basic cybersecurity management systems through cooperation with industry groups and upgrade their capabilities through cyber exercises. For larger FIs the FSA encourages the upgrade of risk management policies and further advance in cybersecurity countermeasures.
Regulatory frameworks	The FSA issued the "Guidelines for Personal Information Protection in the Financial Field". They require FIs and other groups to develop necessary and suitable cybersecurity management measures to prevent data leakage, loss or damage. In addition, the NISC issued the National Strategy for Cybersecurity to improve the cybersecurity of Japanese critical infrastructures encouraging concerned entities to follow cybersecurity best practices.
Cybersecurity culture	The last Cybersecurity Survey shows the following:

	▪ 81% of respondents think that attacks on computer systems is the major threat; ▪ 84% are concerned about cyberattacks.
Cybersecurity education, training and skills	Cybersecurity education and training programs have been created in Japan by government bodies, research/educational institutions: ▪ A program to equip university students with basic skills needed for IT security and cybersecurity; ▪ The Cybersecurity Strategy Headquarters promotes measures to develop security standards, raise awareness and manage and address risks; ▪ The Ministry of Economy, Trade, Industry, and Information-Technology Promotion Agency, have together issued "Cybersecurity Management Guidelines" to urge companies to recognize cybersecurity risks.

4.5. Singapore

Cybersecurity policy and strategy	The Cybersecurity Agency of Singapore (CSA) issued the Cybersecurity Strategy setting out the vision and goals under four pillars: ▪ Increasing resilience of critical information infrastructures; ▪ Mobilizing business to create a cyber-secure environment; ▪ Developing an ecosystem of skilled workforce and technologically-advanced companies; ▪ Forging international partnerships.
Regulatory frameworks	The Monetary Authority of Singapore (MAS) has the mandate to build a cyber-resilient financial sector. In this regard, MAS issued 3 key sets of guidelines and notices: ▪ Technology Risk Management Guidelines; ▪ Notices on Technology Risk Management; ▪ Notices on Cyber hygiene. In addition, the MAS issued a revised Technology Risk Management guidelines to take into account the fast-changing cyber landscape and FI's increasing reliance on cloud computing, APIs and rapid software development. The new guidelines apply to all banks, payment institutions, brokerage and insurance companies.

Cybersecurity culture	The Cybersecurity Awareness Survey showed that: ▪ The level of concern for cyber incidents is high; ▪ Only 4% could identify phishing e-mails; ▪ Many respondents believed that cyber incidents would not happen to them.
Cybersecurity education, training and skills	The Cybersecurity Agency (CSA) provides cybersecurity training and awareness events jointly with public authorities and partners, such as: ▪ Cybersecurity Career Mentoring Program to train and up-skill ICT professionals; ▪ ICE71 is a startup hub aiming to strengthening Singapore's cybersecurity ecosystem; ▪ Singapore Cyber Women Initiative to encourage females to join the cybersecurity profession.

5. Cybersecurity strategy in financial markets

It is critical to define vision, mission and main strategy targets when formulating the scope of the Cybersecurity strategy in financial markets. The vision of the CBA Cybersecurity Strategy is '**to strengthen cyber resilience in financial markets against evolving cyber threats to safeguard financial stability**'.

The mission of the Strategy is **to develop financial system, encompassing a robost security infrastructure in the realm of cybersecurity, developing human capital with advanced knowledge and skills, fostering effective cooperation to facilitate the exchange of information on cyber threats, and establishing adequate regulatory framework to ensure cyber resilience of the financial system.** The main strategic targets of the CBA to accomplish this mission are to **1)** formulate a cybersecurity ecosystem in financial markets of the country, adequately respond to cyber threats and elevate cybersecurity level; **2)** boost financial system resilience by prioritizing continuous information sharing as part of cyber hygiene and mutual partnership; **3)** formulate and update continuously normative-methodological basis related to information security and cybersecurity, thus safeguarding financial stability in financial markets within the mandate of the CBA.

The CBA is planning to realize measures on the following five strategic priorities for 2023-2026 to effectively implement the targets arising from the Strategy:

5.1. Strategic priority 1: Strengthen regulatory and supervisory framework on information security and cybersecurity in financial markets

5.1.1. Formulate risk-based supervisory and regulatory framework

Sophisticated ICT, continuous increase in security risks and intensified information security related incidents (including cyber incidents) are having a considerable effect on activities of FIs. At the same time, as FIs operate in close relation with each other nowadays, critic incidents likely to occur in information security and/or cybersecurity may potentially affect the entire financial system. From this standpoint, financial markets supervisory authorities elaborate related risk-based regulatory and supervisory frameworks and focus on their application.

Application of risk-based regulatory and supervisory frameworks in the financial sector allows to timely detect and assess potential risks FIs may face and determine effective mitigation measures to subdue those risks. Moreover, the aim of risk-based regulation and supervision is to facilitate FIs to better understand supervisory expectations to manage relevant risks. To that end, application of risk-based regulatory and supervisory framework

will help FIs effectively manage risks and test their preparedness against cyber threats and risks they encompass.

With regard to the formulation of risk-based regulation and supervision the CBA expects:

1. FIs adhere to minimum information security requirements, consequently a resilient information security and cybersecurity environment is formed in financial markets;
2. FIs proactively identify cybersecurity risks;
3. Forecast risks emerging in case of changes to cyber threats and threat landscapes and increase confidence that adequate measures can be taken;
4. Take preventive measures before cybersecurity risks become a considerable threat;
5. Elevate cyber resilience of FIs on the back of adjusting cybersecurity regulatory and supervisory framework to international standards and best practices;
6. Reduce the probability and impact of cyber incidents and elevate preparedness of FIs to cyber incidents;
7. Increase trust in the financial sector on the back of improving the reputation of FIs and higher assurance in cyber resilience.

5.1.2. Establishing a sectorial FinCERT in the financial sector

On the back of increasing cyber threats nowadays security vulnerabilities in information systems lead to cybersecurity incidents, thereby disrupting daily business activities of organizations. In a globalized world, the number of multifaceted and technologically diverse attacks against organizations, in particular FIs, that have become targets of various cybercriminals, is increasing. In response to such attacks, organizations develop business continuity and recovery plans in emergencies and test them under various scenarios. Such plans consist of the processes that include actions like detection, assessment, and remediation of security incidents affecting information assets. From the simplest of malware infections to unencrypted laptops that are lost or stolen to compromised login credentials and database exposures, both the short- and long-term ramifications of these incidents can have a lasting impact on the business of any FI.

Taking into account increasing pace of cyberattacks encompassing the financial system, the creation of an incident management platform by the CBA will allow to timely detect, effectively communicate and reduce negative effects of cyber-attacks under current

circumstances. In an international practice the formation of sectorial CERTs, in particular, maintaining relevant activities in the financial system enable to manage relevant incidents, maintain adequate response to incidents, flexible incident notification and planning preventive measures. The main goal of the CERT is to ensure effective management of cybersecurity incidents promptly responding to computer security related incidents.

To discharge its mandated activities the CBA will provide cybersecurity efforts in financial markets by strengthening the legislative base and launch sectorial CERT services to manage cyber risks in the financial system, set adequate supervisory mechanisms and raise awareness. The launch of the incident management center in the CBA will serve to the detection of actions oriented towards disruption of cybersecurity in financial markets, taking measure for their prevention and creating a secure cyber environment in the country with national CERTs as a whole.

The formation of FinCERT in the CBA necessitates the determination of the below three aspects:

- FinCERT mission;
- Possible FinCERT structures;
- Objectives and authorities.

How a CERT is structured depends on the needs of the financial system. Whether 24/7 coverage is needed, availability of human resources with necessary knowledge and skills, operational and investment costs on creation of relevant technological infrastructure and other similar issues. From this standpoint, the main reasons for building FinCERTs are as follows:

- Build a coordinated resilient cybersecurity ecosystem by the creation of FinCERT in financial markets;
- Define the financial system as critical infrastructure as per international practice;
- Collect and investigate either jointly or independently cyber intelligence information of the financial sector and maintain notification using dedicated software;
- Develop response measures against cyber incidents and recovery plans to ensure resilient infrastructure in financial markets;

- Apply cybersecurity requirements and best practices by expanding national and international partnership;
- Strengthen cybersecurity in FIs by forming cyber risk management developments;
- Provide regular cybersecurity trainings under more sophisticated scenarios by attracting stakeholders;
- Provide trainings at FIs to form cybersecurity staff.

5.1.3. FinCERT mission

Delivery of the following services to FIs by FinCERT is considered one of the critical elements of the mission:

1. **Receive an incident report.** In order to receive an incident report from a FI, they first need to know the CERT exists. Stakeholders should also need to be aware of services to be provided by FinCERT and conditions for supply of those services. Thus, the FinCERT needs to define its mission and services, notify stakeholders accordingly and publish guidance on relevant services. To effectively implement functional capacities FinCERT should have relevant infrastructural capacities:
   - FinCERT should act as an umbrella under the legislation and cooperate with national CERTs;
   - Effective communication needs to be organized between FinCERT and national CERTs to strengthen the cybersecurity level in financial markets;
   - To allow FinCERT to adopt best practices in its activities it should launch ties with various international financial CERTs/FS-ISACAs.
2. **Analyze an incident report.** Once an incident report has been received, the FinCERT analyses its reasons. FinCERT then participates in creation of an initial response for recovery of activities and minimizing damage. When reporting to national CERTs on cybersecurity incidents FinCERT should analyse cyber incidents to understand sample threats in the financial system and their impact on the financial system.
3. **Provide support in effective coordination on incident response and investigation of results.** The following needs to be provided depending on the activity direction of FinCERT:

- Support for organization of incident response;
- Coordinate with stakeholders and national CERTs in incident response;
- Initiate raising necessary cybersecurity knowledge and skills and awareness efforts to strengthen cyber resilience in the financial system.

Moreover, FinCERT should promote the creation of the cyber hygiene environment in the financial ecosystem, increase innovations related awareness and focus on this activity continuously. The following needs to be provided as part of this activity:

- Build a sustainable cyber security environment by raising the level of awareness and information on cyber security on a large scale with the involvement of various public and private institutions, as well as by raising the culture of safe use of ICT of every employee in the financial ecosystem;
- Disseminate cybersecurity information through digital channels in close cooperation with national CERTs.

5.1.4. Possible FinCERT structures

Possible CERT structures to be considered by the CBA are the following:

1. Centralized CERT. In a centralized CERT, a single incident response team is created within the organization and the team manages incidents.

2. Distributed CERT. In a distributed CERT, several independent incident response teams exist. The distribution of CERT resources may depend on wide geographic scope of the organization or the location of its major facilities.

3. Coordinating CERT. This CERT manages other, often subordinate, CERTs. This CERT coordinates incident response activities, information flow and workflow among distributed teams. A coordinating CERT may not provide any independent incident response services itself, instead it coordinates activities among distributed teams.

4. Hybrid CERT/SOC. In such a specialized hybrid model, the Security Operations Center (SOC) is kept responsible for obtaining incident notifications and information. In case of the need for additional analysis the SOC activates CERT. SOC detects the event and then transfers it to CERT to be assisted in effective coordination of incident related activities and investigating results.

Having a look at findings of the assessment of cybersecurity stance in financial markets, it was found expedient to apply the **hybrid CERT/SOC** mode. Centralized collection of incidents in financial markets, timely and flexible delivery of incident information to financial ecosystem participants and taking adequate measures will contribute to safeguarding financial system stability.

5.1.5. Roles and responsibilities

Internal organization of the group, as well as clear breakdown of responsibilities among key team members and cross-functional team relationships, is critical. In particular, it is important to organize communication with the supervisory authority of FIs, with technical staff (to collect additional information and investigate issues), as well as with other people (other teams, management and even in some cases law enforcement bodies, media, customers, counterparties, etc.). For this purpose, FIs should at least:

- Develop internal information and cyber security policies, procedures and guidelines to ensure information security.
- Provide special measures, including security incident response and risk management;
- Control the implementation of information security projects in close cooperation with IT and other functional teams;
- Identify current and potential legal and regulatory shortfalls affecting information security and assess their effect with legal and compliance teams;
- Assess information security risks continuously;
- Notify the CBA on information security and cybersecurity incidents likely to have considerable and adverse effect on its capacity to provide adequate services for its customers, its reputation or financial standing;
- Monitor information security in the financial system to manage information security incidents (detect, respond, recover and report).

Creation of a resilient cyber environment, provision of effective coordination, flexible response to incidents and notification of stakeholders will pave the way to reinforcing the current cybersecurity level. On this backdrop, roles and responsibilities of FinCERT should be clearly articulated and communicated to stakeholders.

The following actions are to be conducted over the lifetime of the Strategy:

- determine the policy and the regulatory framework and create safer cyber environment in order to strengthen cybersecurity ecosystem of the financial sector;
- collect, analyze and disseminate information of cyber incidents in financial markets;
- take urgent measures to create a resilient financial sector infrastructure by forecasting, notifying of cyber security incidents likely to occur;
- coordinate cyber incident responses and related activities, and provide methodological support on information security and cybersecurity;
- supervise activities of the financial system on creation of a resilient cybersecurity infrastructure and raise awareness among supervised entities and broad public as a whole;
- provide cybersecurity education measures through digital channels and formulate a cyber-hygiene environment by raising cybersecurity literacy;
- take cybersecurity measures to increase information and cybersecurity culture;
- create an active cooperation framework with national and international CERTs in order to boost cooperation on cybersecurity.

5.2. Strategic priority 2: Strengthening culture of cyber risk management in financial markets

The IT risk management framework should be an integral part of overall operational risk management. The said framework should be comprehensive and support effective assessment of IT risks in FIs. The IT risk management philosophy should be continuous and proactive, and include oversight and supervision of not only technologies, but also humans and processes using technologies in the organization. FIs should apply in-depth elaborated and tested incident response plans and processes in order to reduce the impact of IT incidents and mitigate risks.

CBA's expectations on cyber risks management:

For IT risk management the FI:

1. Develops, applies, continuously updates and communicates the IT risk management framework;

2. Clearly and accurately segregates the roles and responsibilities on services provided by external counterparties, oversees their activities and assesses risks;
3. Analyses, classifies, registers and updates the impact on the business on IT assets;
4. Develops and regularly updates a risk register of IT risks;
5. Prioritizes risks registered in the register to ensure proactive management and record necessary details on risks;
6. Has a structured and documented mitigation plan in place approved and regularly updated by the management to minimize cyber risks;
7. Applies adequate management processes on identification, communication and escalation of IT incidents;
8. Independently checks control mechanisms on IT on an ongoing basis, assesses information security and cybersecurity stance of the organization and provides intrusion tests.

Recovery and business continuity planning:

1. Involve adequate resources on recovery and business continuity planning, testing and application;
2. Elaborate and apply recovery and business continuity plans in order to ensure recovery of it infrastructure and business continuity in the FI in emergencies;
3. Consider various emergencies and incident scenarios, including cybersecurity events when elaborating recovery and business continuity plans in the FI;
4. Create options for continuity of critical operations in accordance with the documented recovery plan during cybersecurity incidents;
5. Develop recovery process(es) of critical information and provide testing of recovery of information from backup copies regularly to test how properly recovery of critical information systems in FIs is implemented;
6. Provide tests on recovery and business continuity plans based upon various scenarios and notify the Board on results regularly.

5.3. Strategic priority 3: Formulating information technologies governance framework to strengthen the level of cybersecurity in financial markets

Internal and external cybersecurity activities of the CBA, in particular maintaining security of critical information systems serving to the support for functions arising from the

mandate of the CBA, including payment, clearing and settlement systems are interconnected. To that end, it is crucial for public-private sectors to have close cooperation ties. Information sharing allows all parties to identify and effectively manage all potential cyber gaps and risks in the financial system. At the same time, this cooperation allows to select adequate response to cyberattacks targeting a certain individual or a wider segment, and determine proper recovery plans on occurred incidents.

Accordingly, the CBA cooperates with financial sector participants operating in the country, and state security authorities responsible for cyber risk management and relevant associations. On an international horizon, the CBA cooperates with a number of central banks to properly harmonize priorities on elevating cybersecurity.

This section includes current development approach and activity directions related to information security and risk management of the CBA. The related initiative of the CBA is to continue activities on depending knowledge and skills to strengthen supervisory and policy frameworks. The CBA will continue open dialogues with FIs and relevant partners with respect to the development and application of the related policy framework. This section consists of three parts: (i) governance; (ii) risk management; (iii) cybersecurity.

The Supervisory Board (Board) approves the information security policy developed in line with goals of the FI and the measures taken to attain these goals as part of the risk management strategy and policy. At the same time, the Board provides effective application of FI's business and IT strategies. In most FIs IT is the main driver that supports critical business functions and pushes business development. Thus, the IT strategy should be comprehensive and support organization's current and future strategic development directions by adapting to the general business strategy.

Moreover, FI's IT risk management framework should be comprehensive, help assess the impact of those risks on business operations effectively and aim to support correct decision-making while mitigating risks affecting critical business operations.

Effective control of IT issues at the Board level and active participation in decision-making paves the way to the formation of a technological and security risk culture in the FI. Thus, having the 'right tone of management' is of particular importance for the formation of the IT risk management culture in the organization.

With respect to the formation of the IT governance framework the CBA expects:

1. The FI to develop and approve a comprehensive IT strategy that is aligned with the overall business strategy;
2. Allocate adequate resources, including budget, staff levels and skills to implement a business-aligned IT strategy;
3. Regular reports are submitted to the Board on necessary issues, priorities, as well as information security incidents and risks when implementing strategic IT initiatives;
4. The Board as a whole and Senior Management possess sufficient knowledge and understanding of the IT related risks facing the FI and those risks are properly managed and communicated to the supervisory authority.
5. The FI has an adequate IT management structure to effectively manage IT risks;
6. The FI has documented IT policy, procedures and regulations;
7. The FI clearly defines roles and responsibilities for IT risk management, including decision-making in emergency and crisis situations, and effectively communicates to relevant parties;
8. Local representative offices of foreign FIs align IT strategies and management frameworks adopted by foreign FIs to the legislation of Azerbaijan and regulations determined by the supervisory authority;
9. Assurance on effective organization of IT risk management, internal control and overall management processes by the FI's management structure.

5.4. Strategic priority 4: Strengthening cyber resilience in financial markets

FIs are increasingly exposed to cyber-attacks, since cyberattacks are more frequent, more targeted and progressively more difficult to detect and mitigate relevant risks. In addition, current and long-term technological trends (such as cloud computing, "big data", mobile devices, financial technology and "the internet of things") will further increase exposure to cyber risk. Technical complexities of the risks arising from operating in the digital society, with organizations required to manage a multiplicity of interrelated risks and vulnerabilities, pose significant challenges. FIs should apply adequate mitigation-control processes in place to effectively address cyber risk. While it is recognised that there is no 'one size fits all' solution to addressing these threats, all FIs should pre-analyze negative

effect and implications of cyberattacks. The cyber risk management elements of the IT risk management framework, including associated policies and procedures, should not be viewed as static. Hence, FIs should review and update relevant frameworks regularly to reflect threat intelligence and changes in the internal and external operational environment to proactively avoid security threats. FIs can reduce frequency of security incidents by actively maintaining the security of information systems, hardware and software, data and network systems. Adverse impacts arising from security incidents can be lessened by maintaining adequate incident handling capabilities and ensuring that incident recovery plans are in place. Further, poor security awareness in a FI is a significant contributor to increased cyber risk. Awareness can be increased through training and continuous reinforcement of users' security responsibilities and by the promotion of a strong security culture throughout the FI.

With regard to cybersecurity, the CBA expects that:

1. Cyber risk is managed within the context of overall IT risk management;
2. FIs have a well-considered and approved procedures and regulations in place to support the effective management of information and cyber security risks;
3. Cybersecurity roles and responsibilities are defined, documented and communicated to relevant parties within the institution;
4. The FI develops and implements information security awareness training programs;
5. At a minimum, cyber risk management addresses:
   - the identification of threats, vulnerabilities and risks and assessment of exposure to the FI;
   - the prevention and detection of security events and incidents and adequate response, including effective management of incidents when they occur;
   - recovery planning for stabilization and continuity of operations in the immediate aftermath of a security incident, if necessary.
6. Cyber risk assessments are performed on a regular basis with the identification of external and internal threats.
7. Robust safeguards are in place to avoid cybersecurity events and incidents;
8. Processes on classification of information (as well as personal information) stored, processes and transmitted at the FI are developed, applied and updated, at the same

time, confidential and open information is properly identified and adequate security measures are applied;

9. Internal and external access control to information systems of the FIs in place;
10. Information systems and assets control mechanisms are in place, predictive indicators are applied to detect security events and incidents in a timely manner and effectiveness of detection processes and procedures are tested periodically;
11. FIs conduct intrusion tests both at the expense of internal resources and reliable external counterparties;
12. Develop and apply responses and recovery plans consisting of systematic and overwhelming measures during the security incident recorded at the FI;
13. Formulate the knowledge base based on findings identified because of cybersecurity incidents, update incident response and recovery plans continuously.

5.5. Strategic priority 5: Formulating information security and cybersecurity culture in financial markets

Continuous development of the cyber and information security culture has become one of the crucial directions of the ever-digitalizing financial-banking sector. To make introduced services more available, FIs increasingly prioritize technologies, which makes them more sensitive to cyber risks on the back of rising cyber threats and attacks. In its turn, it may lead to financial and reputation loss and customer distrust. To that end, to protect customer information (including personal information) at financial markets and prevent financial frauds it is very important to take proactive measures on information and cyber security.

In this context, the CBA plays a crucial role in FIs' building effective cybersecurity practices and compliance with relevant regulations and standards. The CBA will cooperate with FIs to accelerate cybersecurity measures at financial markets and shape a robust information security culture. As part of related efforts the CBA is planning to build strong cyber hygiene practices in close communication with FIs and related authorities; conduct cybersecurity awareness programs; develop experts trained and certified on cybersecurity; and provide other security measures. Consequently, FIs will be able to elevate confidence in the financial system and create a secure environment promoting trust meeting these expectations.

With regard to the formation of information and cybersecurity culture the CBA expects that:

1. Effective coordination with FIs and related authorities to identify cyber threats and minimize their effects;
2. Create a strong cyber hygiene environment to maintain financial system stability;
3. Provide programs and initiatives to raise cybersecurity awareness of staff and customers at FIs;
4. Develop cybersecurity experts trained and certified on relevant areas to maintain cyber resilience of the financial sector;
5. Study insurance practices against cybersecurity incidents and assess probability of their application to increase confidence in financial services at financial markets.

6. Expected outcome

The effective implementation of the measures specified under the strategy will allow **1)** strengthening financial sector stability, **2)** developing cooperation and communication in implementing cyber security measures, **3)** intensifying the application of cybersecurity measures in FIs and shaping relevant skills and **4)** taking proactive cybersecurity measures on prevention of cyber threats. Expected outcome as part of the implementation of the Strategy is as follows:

- The CBA will ensure strengthening of financial system stability by implementing cybersecurity resilience measures within the frames of cooperation;
- Cybersecurity risks in the financial system of the country will be identified, analyzed and documented, and adequate response mechanisms will be applied to reduce cyber risks;
- A cooperation will be built with national and international partners to properly identify, communicate and manage cybersecurity risks in the financial sector of the country;
- An effective risk-based supervisory framework for financial market participants will be shaped to maintain financial system stability. Cyber stability will be boosted by applying cybersecurity policies and regulatory initiatives;
- The CBA will apply adequate response to cyber threats arising from dynamically intensified digitalization trends and develop private and public partnership to that end.

As part of the implementation of the Strategy, the CBA will conduct annual surveys based on international standards and cyber security framework documents and assess the cyber security stance at financial institutions. The cybersecurity maturity level of financial market participants is planned to reach relevant target indicators.

Table 2: Cybersecurity key performance indicators

№	Financial market segments	Current indicators	Target indicators (2026)
1	**Banking sector**[10]	2.14	3.5
1.1	*Including systemically important banks*	*3.08*	*3.7*
2	**Insurance sector**[11]	1.85	2.5
3	**Capital markets**[12]	-	2.5
4	**Payments market**[13]	2.85	3.5
Total indicator on financial markets		**2.28**	**3.0**

Strategic priorities, measures, and outcome indicators to be implemented as part of the Strategy are included to the Actions Plan.

[10] *Banks, non-bank credit institutions*

[11] *CIB, insurers*

[12] *Stock exchange, clearing organization, investment companies*

[13] *Payment system operators, electronic money organizations. This indicator will start to be measured once the payment services and payment systems legislaiton is formulated.*

7. Actions Plan on cybersecurity strategy in financial markets

№	Actions	Implementation period	Responsible party(ies)	Outcome indicators		
				Initial result(s)	Interim result(s)	Outcome
Strategic priority 1: Strengthening regulatory and supervisory framework on information security and cybersecurity in financial markets						
1.1	**Formulation of the risk-based regulatory and supervisory framework**					
1.1.1	Expand the scope of information security management regulations	2023-2024	CBA	Study international practice	Formulate minimum information security requirements for FIs	
1.1.2	Assess and report maturity of the cybersecurity stance of financial markets	2023-2026	CBA	Create the risk-based supervisory framework	Conduct comprehensive and thematic inspections	Assess maturity level and develop reports
1.2	**Create sectorial CERT (FinCERT) on financial markets as part of safeguarding cyber stability**					
1.2.1	Formulate a procedure for the development and submission of incidents by FIs	2023-2024	CBA	Formulate procedure for the development and reporting of incidents by FIs		
1.2.2	Create an incident sharing system in financial markets	2024-2026	CBA, FIs	Designate coordinators responsible for submission of incidents	Create and commission the system	Formulate a knowledge base on incidents
1.2.3	Formulate a sectorial CERT (FinCERT) on financial markets	2023-2025	CBA	Improve the legislative base	Take institutional measures within the organization	Establish FinCERT
1.2.4	Analyze cyber threats in financial markets	2024-2025	CBA, FIs	Assess options for introduction of technical tools on cyber threat intelligence		

Strategic priority 2: Strengthening culture of cyber risk management in financial markets						
2.1	Formulate an internal risk management framework covering cyber risks	2024-2026	FIs	Formulate a risk management framework and determine cyber risk appetite	Maintain self-assessment to control risks	Determine internal cyber risks and formulate response strategies
2.2	Classify information system in line with the level of their criticality	2024-2026	FIs	Analyze business impact	Formulate a register	Update register
2.3	Ensure business continuity in emergency situations	2024-2026	FIs	Develop business continuity and recovery plans	Test business continuity and recovery under various scenarios	
Strategic priority 3: Formulating information technologies governance framework to strengthen the level of cybersecurity in financial markets						
3.1	Formulate an internal IT strategy supporting business-aligned development targets	2023-2024	FIs	Develop, approve and implement an IT strategy		
3.2	Develop IT governance procedures and regulations	2024-2026	FIs	Document and apply IT governance processes		
Strategic priority 4: Strengthening cyber resilience in financial markets						
4.1	Build resilient information systems protected against cyber-attacks and threats	Regularly	FIs	Build protection systems up to modern requirements	Introduce a ‘zero trust’ policy	Regularly update protection systems
4.2	Maintain incident management activities	2024-2026	FIs	Develop policies and procedures	Monitor and report incidents	Submit incident information to related organizations
4.3	Maintain system logs management activities	2024-2026	FIs	Develop policies and procedures	Ensure continuity of activities	
4.4	Maintain vulnerabilities management activities	2024-2026	FIs	Develop policies and procedures	Ensure continuity of activities	

4.5	Maintain intrusion (penetration) testing	2024-2026	FIs	Develop policies and procedures	Ensure continuity of activities	
4.6	Form an experienced human capital on cyber security	Regularly	FIs	Establish and conduct related training programs		Train certified specialists in the relevant field
Strategic priority 5: Formulating information security and cybersecurity culture in financial markets						
5.1	Strengthen coordination on information security and cybersecurity in financial markets	2023	CBA, associations, FIs	Create a working group of persons responsible for information and cyber security		
5.2	Launch cooperation with national and international CERTs	Regularly	CBA, national and international organizations	Formulate a cooperation framework with CERTs		
5.3	Formulate a cyber-hygiene environment in financial markets	Regularly	CBA, associations, national and foreign organizations, FIs	Set priority directions on awareness	Conduct cybersecurity round tables	Conduct awareness events
5.4	Implement cybersecurity and acceleration programs	Regularly	CBA, associations, national and foreign organizations, FIs	Hold cybersecurity forums		Implement acceleration programs (hackathon, bootcamp etc.)
5.5	Promote insurance against cybersecurity incidents in financial markets	2024-2026	CBA, associations, relevant FIs	Study international practice on the creation of an insurance mechanism		Promote insurance against cybersecurity incidents

8. Time table on implementation of the cybersecurity strategy in financial markets

№	Actions	2023				2024				2025				2026			
		I	II	III	IV	I	II	III	IV	I	II	III	IV	I	II	III	IV
Strategic priority 1: Strengthening regulatory and supervisory framework on information security and cybersecurity in financial markets																	
1.1	**Formulation of risk-based supervisory and regulatory framework**																
1.1.1	*Expand the scope of information security management regulations*																
	Study international practice																
	Formulate minimum information security requirements for FIs																
1.1.2	*Assess and report the maturity level on the cybersecurity stance of financial markets*																
	Create a risk-based supervision framework																
	Conduct comprehensive and thematic inspections																
	Assess maturity level and develop reports																
1.2	**Create sectorial CERT (FinCERT) on financial markets as part of safeguarding cyber stability**																
1.2.1	*Formulate a procedure for development and submission of incidents by FIs*																
	Formulate procedure for the development and reporting of incidents by FIs																
1.2.2	*Create an incident sharing system in financial markets*																
	Designate a coordinator responsible for submission of incidents																

	Create and commission the system																
	Formulate a knowledge base on incidents																
1.2.3	*Form a sectorial CERT (FinCERT) on financial markets*																
	Improve the legislative base																
	Take institutional measures within the organization																
	Establish FinCERT																
1.2.4	*Analyze cyber threats in financial markets*																
	Assess options of introduction of technical tools on cyber threat intelligence																
Strategic priority 2: Strengthening culture of cyber risk management in financial markets																	
2.1	**Formulate an internal risk management framework covering cyber risks**																
	Formulate a risk management framework and determine a cyber-risk appetite																
	Maintain self-assessment to control risks																
	Determine internal cyber risks and formulate response strategies																
2.2	**Classify information systems in line with the level of their criticality**																
	Analyze business impact																
	Formulate a register																
	Update register																
2.3	**Ensure business continuity in emergency situations**																

	Develop business continuity and recovery plans																	
	Test business continuity and recovery under various scenarios																	
Strategic priority 3: Formulating information technologies governance framework to strengthen the level of cybersecurity in financial markets																		
3.1	**Formulate an internal IT strategy supporting business-aligned development targets**																	
	Develop, approve and implement an IT strategy																	
3.2	**Develop IT governance procedures and regulations**																	
	Document and apply IT governance processes																	
Strategic priority 4: Strengthening cyber resilience in financial markets																		
4.1	**Build resilient information systems protected against cyber-attacks and threats**																	
	Build protection systems up to modern requirements																	
	Introduce a ‘zero trust’ policy																	
	Regularly update protection systems																	
4.2	**Maintain incident management activities**																	
	Develop policies and procedures																	
	Monitor and report incidents																	
	Submit incident reports to related organizations																	
4.3	**Maintain system log management activities**																	
	Develop policies and procedures																	

	Ensure continuity of activities																	
4.4	**Maintain vulnerabilities management activities**																	
	Develop policies and procedures																	
	Ensure continuity of activities																	
4.5	**Maintain intrusion (penetration) testing**																	
	Develop policies and procedures																	
	Ensure continuity of activities																	
4.6	**Form an experienced human capital on cyber security**																	
	Establish and conduct relevant training programs																	
	Train certified specialists in the relevant field																	
Strategic priority 5: Formulating information security and cybersecurity culture in financial markets																		
5.1	**Strengthen coordination of information security and cybersecurity in financial markets**																	
	Create a working group of persons responsible for information and cyber security																	
5.2	**Launch cooperation with national and international CERTs**																	
	Formulate a cooperation framework with CERTs																	
5.3	**Formulate a cyber-hygiene environment in financial markets**																	
	Set priority directions on awareness																	
	Conduct cybersecurity round tables																	

	Conduct awareness events																	
5.4	**Implement cybersecurity and acceleration programs**																	
	Hold cyber security forums																	
	Implement acceleration programs (‘hackathon’, ‘boot camp’ etc.)																	
5.5	**Promote insurance against cybersecurity incidents in financial markets**																	
	Study international practice on the creation of an insurance mechanism																	
	Promote insurance against cybersecurity incidents																	