Ahmet Ismaili: Cybersecurity in the banking industry

Speech by Mr Ahmet Ismaili, Governor of the Central Bank of the Republic of Kosovo, at the Conference "Cybersecurity in the banking industry", co-organised by the Kosovo Banking Association and the Albanian Association of Banks, Pristina, 25 October 2023.

* * *

Dear Mr Balija, Chief Executive Officer of the Kosovo Banking Association

Dear Mr Brumbulli, Secretary General of the Albanian Association of Banks

Dear Mr Bakkal, Chairman of the Board of Directors of the Kosovo Banking Association

Dear, Mrs Hoxha, Senior Investment Officer at Finance in Motion (EFSE)

Dear Members of Bank Associations

Dear Board Members

Dear panellists and attendees

I am pleased to greet and welcome you all to the "Cybersecurity in the Banking Industry" Conference, co-organized by the Kosovo Banking Association and the Albanian Association of Banks.

The very fact that we have co-organization shows the excellent cooperation between the banking sectors of our two countries, but also the approach to the common challenge, which knows no borders. Therefore, my participation here today also aims to convey such a message of coordination and joint efforts to address these risks, as one of the most complex challenges of the time for the financial industry and beyond.

We are witnessing the time that the financial system is changing quite quickly and is being transformed. Digitization on the one hand has influenced the improvement of access to services as well as their quality, which means that in the field of payments, services are being carried out continuously and are available worldwide.

But, on the other hand, the main risks related to the introduction of information technology that enables banking and financial services have increased and constitute a threat to be handled with care. They include strategic and reputational risk, operational risk, cyber risk and compliance risk.

The cyber threat continues to evolve and become more complex amid continued digitization, increased third-party dependencies, and geopolitical tensions.

The rapid pace of technological advancement imposes the need for continuous monitoring of emerging trends and their possible impacts on the operations of financial institutions.

Therefore, strengthening cyber security in the financial sector is a priority for financial stability, and not only that. Its influence extends to national security.

The Republic of Kosovo, through the National Security Strategy, has determined the responsibilities and duties of the institutions for cyber security and critical infrastructure, from the coordination of legal and strategic initiatives to the development of their protective capacities and functions.

In this sense, since the Central Bank of the Republic of Kosovo, according to its mandate, maintains the health of the banking and financial system in general, it recognizes and addresses with increased care the aspects of cyber security and the risks arising from them.

The CBK recognizes the critical importance of information systems and cyber security in the financial sector and as a proactive measure to maintain the stability and integrity of financial institutions.

We are committed to advancing the regulatory and supervisory framework for financial institutions in harmony with European Union Regulations and Directives as well as international standards and best practices in this field.

As for internal capacities and organization, with the new organizational chart, we will create a structure dedicated to the supervision of information systems or cyber risk.

Investment will be made in building infrastructural capacities and human resources to ensure that systems, equipment, knowledge, skills and tools of the personnel remain relevant and effective in overseeing the risks of new technologies and innovative business models.

The main objectives such as increasing cyber resilience, mitigating operational risks, establishing and implementing cyber security standards, performing comprehensive risk assessments, ensuring effective response to incidents, etc., will be addressed through regulatory instruments and mechanisms, such as cyber security standards, compliance requirements, alignment with international standards, incident response plan and others.

The strengthening of internal capacity will be based on support through technical assistance from the IMF's specialized team, who will help design the strategic framework, policies and procedures according to the best world standards.

Their principles will also be applicable to the entire sector, through a constructive and regulatory and advisory partnership with financial institutions.

In this sense, we as CBK expect the banking industry to:

- Have effective governance structures and risk management processes;
- Address cyber risk through specific strategies, policies and procedures that include requirements related to governance and oversight, risk ownership and accountability, information security, etc.;

- Have adequate risk management practices and processes when dealing with outsourced services, which include due diligence, operational risk management, ongoing monitoring and proper execution of contracts with outsourced service providers that define the responsibilities of each party;
- Invest in infrastructure and have sufficient qualified personnel to monitor and supervise their activities contracted by third parties; and
- Take into account factors that ensure business continuity, confidentiality and integrity of information when contracting services from external parties, as well as increase attention to external ownership and origins of funds to clients, through Investor's Screening Mechanism, given the current geostrategic risks.

Finally, we remind you that addressing cyber risks requires close cooperation between different authorities, with an emphasis on the state authorities responsible for cyber security at the state level.

The CBK remains committed to coordinating and sharing information with other regulators, relevant public authorities such as those for data protection, consumer protection, competition and national security institutions.

At the same time, also in the international aspect, with international institutions, regulators of the countries of the region, other institutions, with the aim of coordination and a more stable platform to successfully face these risks and achieve our objectives.

We wish you fruitful discussions in the following panels, and we welcome the recommendations resulting from these professional discussions.

Thank you!