KINSTELLAR

Managing ICT Risks in the Financial Sector

Information and communication technology ("**ICT**") is integral to the functioning of the financial sector of modern economies. In recent decades, ICT has become a critical aspect of the daily functions and operations of financial entities. Such high degree of dependence on ICT systems constitutes a systemic vulnerability, due to the interconnected nature of the global economy. Recognising this risk, international regulatory organisations have worked to equip competent authorities and market participants with the necessary tools to strengthen the resilience of their financial systems. These circumstances highlight the need for governments to take appropriate measures to address ICT-related risks through special legislation, even at the expense of additional administrative burdens to private entities. This newsletter presents the measures taken to address these risks across Kinstellar's jurisdictions.

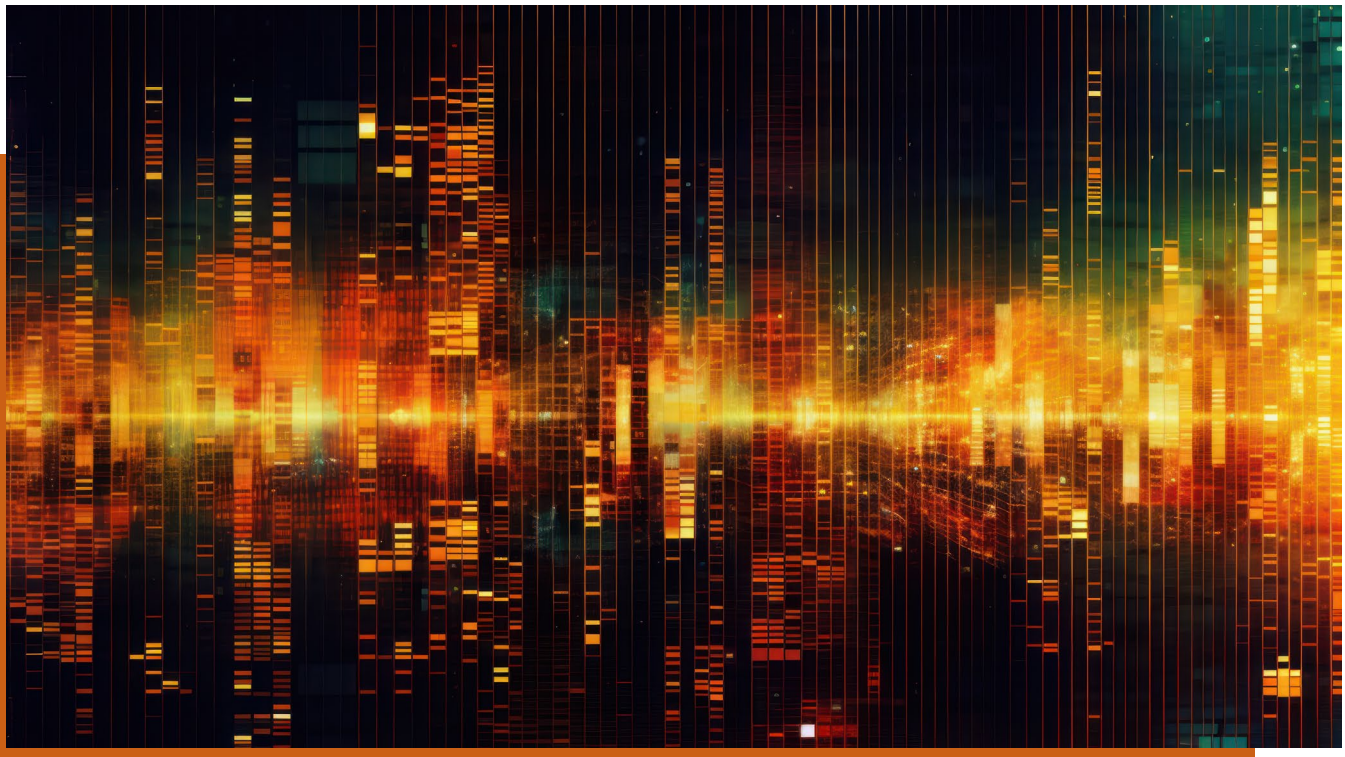


Table of contents

Information current as of June 2025. It is for general informational purposes only and does not constitute legal, professional or investment advice. For specific guidance or expert consultation, please contact our team.

BULGARIA

01 | Main legislation regulating operational resilience for the financial sector

The primary legal instrument regulating ICT risks in the financial sector in the EU is Regulation (EU) 2022/2554 of the European Parliament and of the Council ("**DORA**" or the "**Regulation**"). It was officially adopted in 2022 and is applicable as of 17 January 2025. DORA applies directly in all Member States, and its provisions will be additionally implemented in Bulgaria through amendments to national legislation.

Two proposed draft bills will make the necessary changes to existing legislation. Upon their entry into force, the operational resilience of the financial sector in Bulgaria will be regulated by several acts, including the Markets in Crypto Assets Act; the Payment Services and Payment Systems Act; the Credit Institutions Act; the Bulgarian National Bank ("**BNB**") Act; the Financial Supervision Commission ("**FSC**") Act; the Public Offering of Securities Act; the Collective Investment Schemes and Other Undertakings for Collective Investments Act; the Social Insurance Code; the Insurance Code; the Recovery and Resolution of Credit Institutions and Investment Firms Act, and the Markets in Financial Instruments Act.

The list of applicable national instruments may be further expanded by future amendments to different legislative and administrative acts.

02 | Who needs to comply?

The obligations related to the operational resilience of the financial sector apply to finance-related institutions and financial entities, which can be grouped as follows:

- credit institutions, payment institutions, crypto-asset service providers, and electronic money institutions;
- central securities depositories, securitisation repositories, central counterparties, trading venues, trade repositories, data reporting service providers, and account information service providers;
- managers of alternative investment funds, credit rating agencies, crowdfunding service providers, institutions for occupational retirement provisions, management companies; and
- ICT third-party service providers.

03 | Who are the responsible regulators?

According to the proposed draft bills, the responsible regulators will be the BNB and the FSC. Each body will have separate regulatory competences.

The BNB will be competent in relation to credit institutions, payment institutions, and administrators of critical benchmarks. The FSC will be competent in relation to investment firms, crypto-asset providers, central securities depositories, insurers, institutions for occupational retirement provision, and others.

The BNB will also appoint a member of its staff to be a high-level representative in the Oversight Forum, which assists in EU-wide control.

04 | What are the key requirements?

DORA identifies ICT risk management, incident reporting, operational resilience testing, third-party risk management, and cyber-threat intelligence sharing as the main pillars of the operational resilience framework.

Financial entities need to deploy appropriate strategies, policies, procedures, protocols, and tools in relation to ICT-risk management. The functions and roles related to ICT should be identified, classified, and adequately documented. Sources of ICT risk should be reviewed on a regular (at least yearly) basis. Major changes to network and information system infrastructure should always be performed after prior risk-exposure assessment.

Overall, the risk-management framework is centred around protection and prevention, detection, response and recovery, and learning and evolving.

The Regulation's requirements related to incident reporting obliges financial entities to manage and notify ICT-related incidents. Such incidents are classified based on certain criteria and reported to the competent authorities. A unified reporting format will be created by the European Supervisory Authorities.

The digital operational resilience of financial entities will be tested (at least yearly), so as to assess its preparedness. The testing program will include a range of assessments, tests, methodologies, practices, and tools. The appropriate tests can take the form of vulnerability assessments and scans, open-source analyses, network security assessments, and scenario-based tests, among others. Critical financial firms must conduct Threat-Led Penetration Testing at least every three years.

Before financial entities enter into a contractual arrangement with external ICT service providers, they should perform certain mandatory compliance checks. There are also mandatory contract clauses (e.g., that the contract may be terminated in case of a significant breach of applicable laws by the service providers). The European Supervisory Authorities will designate certain external ICT providers as critical.

Financial entities are encouraged to exchange cyber-threat information and intelligence among themselves. Such information sharing should be aimed at raising awareness within trusted communities of financial entities.

05 | What steps and actions should be undertaken?

The first step towards meeting the requirements described in the previous answer is conducting a gap analysis to assess current practices and identify the potential areas for improvement.

Financial entities should strengthen their internal governance structures by assigning clear roles and responsibilities for ICT risk management.

Risks arising from third-party relations should be addressed by reviewing vendor contracts and establishing mandatory security requirements.

Protocols for incident reporting should be developed to ensure timely and accurate responses.

A cyber intelligence-sharing mechanism for ensuring collaboration with government bodies and industry peers should be established.

An ongoing step is educating employees and management of the regulatory requirements and best cybersecurity practices to improve organisational awareness.

06 | What are the sanctions?

Financial entities that violate the requirements will be sanctioned by the BNB or FSC in the amount of BGN 20,000 to BGN 40,000 (approx. EUR 10,000 to EUR 20,000). In second cases of violations, the sanctions are increased to BGN 40,000 to BGN 100,000 (approx. EUR 20,000 to EUR 50,000).

Representatives of financial entities (i.e., natural persons) can be fined by the BNB or FSC in their personal capacity if they violate the requirements or allow such a violation. The fines range from BGN 10,000 to BGN 20,000 (approx. EUR 5,000 to EUR 10,000). Second cases of violations can lead to fines in the range of BGN 20,000 to BGN 40,000 (approx. EUR 10,000 to EUR 20,000).

Svilen Issaev
Counsel

+359 2 9048 361
svilen.issaev@kinstellar.com

Nikolay Gergov
Senior Associate

+359 2 9048 363
nikolay.gergov@kinstellar.com

CROATIA

01 | Main legislation regulating operational resilience for the financial sector

The main legislation governing operational resilience for the financial sector is the EU's Digital Operational Resilience Act ("DORA"), established by Regulation 2022/2554/EU on digital operational resilience.

The Regulation is complemented by various implementing and delegated acts that provide further guidance and details on specific aspects of the Regulation. A full list of these implementing and delegated acts can be found here.

In addition to EU legislation, national legislation has been adopted in Croatia to implement DORA into Croatian law. i.e., the Act on the Implementation of Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector ("DORA Implementing Act").

02 | Who needs to comply?

DORA applies to a broad spectrum of financial entities as well as to certain ICT third-party service providers. Specifically, it directly covers financial entities including:

- banks and other credit institutions;
- insurance and reinsurance firms;
- investment firms;
- payment service providers;
- crypto-asset service providers.

In addition to these entities, DORA also has implications for ICT third-party service providers—such as cloud computing or data analytics providers—if they offer services to financial entities.

Notably, ICT third-party service providers that are deemed critical may be formally designated as such by the European Supervisory Authorities (EBA, ESMA, or EIOPA). Once designated, these ICT third-party service providers fall under direct supervision within the DORA framework.

DORA does not apply to credit unions or to Croatian Bank for Reconstruction and Development.

03 | Who are the responsible regulators?

The Croatian National Bank ("HNB") and Croatian Agency for the Supervision of Financial Services ("HANFA") are the competent authorities under the DORA Implementing Act.

HNB is the competent authority for:

— credit institutions;

— payment institutions;

— account information service providers;

— electronic money institutions;

— issuers of asset-referenced tokens.

For other entities, the competent authority is HANFA.

04 | What are the key requirements?

DORA is structured around five key pillars:

I. ICT Risk Management – Businesses must implement strong cybersecurity measures, conduct regular security testing, and involve senior management in ICT risk governance.

II. Incident Reporting – Companies must detect, classify, and report significant ICT-related incidents promptly using a standardised format. The European Supervisory Authorities will create a unified reporting format.

III. Digital Operational Resilience Testing – Companies must conduct regular penetration testing, vulnerability assessments, and scenario-based exercises. Critical financial firms must conduct Threat-Led Penetration Testing at least every three years.

IV. ICT Third-Party Risk Management – Enhanced oversight of external ICT service providers, including mandatory contractual obligations and compliance checks. The European Supervisory Authorities will designate certain ICT providers as critical.

V. Cyber Threat Intelligence Sharing – Encourages collaboration across the financial sector to improve cybersecurity defenses.

05 | What steps and actions should be undertaken?

1. Conduct a gap analysis to assess current ICT risk management practices and identify areas for improvement.
2. Strengthen governance structures by assigning clear roles and responsibilities for ICT risk management.
3. Strengthen third-party risk management by reviewing vendor contracts and establishing mandatory security requirements.
4. Develop an incident reporting protocol aligned with DORA's reporting requirements to ensure timely and accurate reporting.
5. Implement regular cybersecurity testing, including penetration testing, scenario-based exercises, and operational resilience drills.
6. Establish cyber intelligence sharing mechanisms to collaborate with industry peers and regulators on emerging threats.
7. Educate employees and management on DORA's requirements and cybersecurity best practices to improve organisational awareness.

06 | What are the sanctions?

CNB and HANFA can issue supervisory measures as follows:

- order supervised entities and responsible persons to cease and desist from behaviour that violates DORA;
- request a temporary or permanent cessation of actions or behaviour deemed contrary to DORA and prevent their recurrence;
- impose or determine measures in accordance with DORA and file charges to ensure supervised entities comply with these regulations;
- request existing telecommunication operator records on data traffic;
- issue public announcements.

Companies may face significant sanctions for breaching obligations under DORA. The DORA Implementing Act provides for administrative fines of up to 3% of total annual turnover, including at the consolidated level. Responsible individuals and management members of companies can also be fined up to EUR 15,000.

Additionally, sanctions decisions are publishable on CNB's or HANFA's websites.

Edin Karakaš
Partner

+385 1 5555 663
edin.karakas@kinstellar.com

Marija Vuchetich
Counsel

+385 1 5555 670
marija.vuchetich@kinstellar.com

CZECH REPUBLIC

01 | Main legislation regulating operational resilience for the financial sector

The main legislation governing operational resilience for the financial sector in the Czech Republic is the EU's Digital Operational Resilience Act ('DORA"), established by Regulation 2022/2554/EU on digital operational resilience.

The Regulation is complemented by various implementing and delegated acts that provide further guidance and details on specific aspects of the Regulation. A full list of these implementing and delegated acts can be found here.

In addition to the EU legislation, national legislation has been adopted in the Czech Republic to implement DORA into Czech law, namely:

- Czech Act No. 31/2025 Coll., on the implementation of European Union regulations in the area of financial market digitalisation; and
- Czech Act No. 32/2025 Coll., amending certain acts in connection with the implementation of European Union regulations in the area of the digitalisation of the financial market and sustainability financing.

02 | Who needs to comply?

DORA applies to a broad spectrum of financial entities as well as to certain ICT third-party service providers. Specifically, it directly covers financial entities including:

- banks and other credit institutions;
- insurance and reinsurance firms;
- investment firms;
- payment service providers;
- crypto-asset service providers.

In addition to these entities, DORA also has implications for ICT third-party service providers—such as cloud computing or data analytics providers—if they offer services to financial entities.

Notably, ICT third-party service providers that are deemed critical may be formally designated as such by the European Supervisory Authorities (EBA, ESMA, or EIOPA). Once designated, these ICT third-party service providers fall under direct supervision within the DORA framework.

03 | Who are the responsible regulators?

The Czech National Bank ("ČNB") is the competent authority under DORA.

As the regulatory authority for the financial sector, the Czech National Bank cooperates with the National Cyber and Information Security Agency ("NÚKIB") in overseeing cyber and information security in the financial sector.

04 | What are the key requirements?

DORA is structured around five key pillars:

I. ICT Risk Management – Businesses must implement strong cybersecurity measures, conduct regular security testing, and involve senior management in ICT risk governance.

II. Incident Reporting – Companies must detect, classify, and report significant ICT-related incidents promptly using a standardised format. The European Supervisory Authorities will create a unified reporting format.

III. Digital Operational Resilience Testing – Companies must conduct regular penetration testing, vulnerability assessments, and scenario-based exercises. Critical financial firms must conduct Threat-Led Penetration Testing at least every three years.

IV. ICT Third-Party Risk Management – Enhanced oversight of external ICT service providers, including mandatory contractual obligations and compliance checks. The European Supervisory Authorities will designate certain ICT providers as critical.

V. Cyber Threat Intelligence Sharing – Encourages collaboration across the financial sector to improve cybersecurity defences.

05 | What steps and actions should be undertaken?

1. Conduct a gap analysis to assess current ICT risk management practices and identify areas for improvement.
2. Strengthen governance structures by assigning clear roles and responsibilities for ICT risk management.
3. Strengthen third-party risk management by reviewing vendor contracts and establishing mandatory security requirements.
4. Develop an incident reporting protocol aligned with DORA's reporting requirements to ensure timely and accurate reporting.
5. Implement regular cybersecurity testing, including penetration testing, scenario-based exercises, and operational resilience drills.
6. Establish cyber intelligence sharing mechanisms to collaborate with industry peers and regulators on emerging threats.
7. Educate employees and management on DORA's requirements and cybersecurity best practices to improve organizational awareness.

06 | What are the sanctions?

Financial entities and ICT third-party service providers may face significant sanctions for breaching obligations under DORA. The sanctions are set out in Czech Act No. 31/2025 Coll., on the implementation of European Union regulations in the area of financial market digitalisation.

The Act provides for administrative fines of up to:

- CZK 50 million (approx. EUR 2 million) for serious breaches (e.g., failures in ICT risk management, continuity planning, or resilience testing);
- CZK 20 million (approx. EUR 800,000) for other material breaches (e.g., failure to properly classify ICT incidents or improper ICT incident management); and
- CZK 10 million (approx. EUR 400,000) for less severe offences (e.g., reporting failures or lack of cooperation with supervisors).

Additionally, the Czech National Bank may order publication of the sanction decision.

Sanctions also apply to ICT third-party service providers, including critical providers, particularly for failing to cooperate with the supervisory authority.

Martina Březinová
Counsel
+420 221 622 229
martina.brezinova@kinstellar.com

Jakub Šťastný
Managing Associate
+420 221 622 276
jakub.stastny@kinstellar.com

HUNGARY

01 | Main legislation regulating operational resilience for the financial sector

The primary legislation governing the operational resilience of the financial sector in Hungary, as an EU Member State, is Regulation (EU) 2022/2554 on digital operational resilience for the financial sector ("DORA"), which, together with the associated Regulatory Technical Standards ("RTS") and Implementing Technical Standards ("ITS"), is directly applicable in Hungary.

During the preparatory phase for the implementation of DORA, all key domestic legislative acts governing the financial sector—namely the Credit Institutions Act, the Investment Services Act, the Act on the National Bank of Hungary, and the Capital Market Act—were amended to align with the provisions of DORA.

In addition to these statutory legislations, the National Bank of Hungary ("NBH"), in its capacity as a regulator, has revised several of its supervisory guidelines to support compliance with DORA. Notable examples include the updated Information Security Recommendation, addressing the protection of IT systems, and the Cloud Services Recommendation, which provides guidance on the use of community and public cloud services. Further updates to NBH recommendations are expected.

02 | Who needs to comply?

DORA applies to a wide range of entities operating within the financial sector. Specifically, its scope extends to the following entities:

- credit institutions;
- payment institutions;
- account information service providers;
- electronic money institutions;
- investment firms;
- crypto-asset service providers authorised under the Markets in Crypto Assets Regulation, including issuers of asset-referenced tokens;
- central securities depositories;
- central counterparties;
- trading venues;
- trade repositories;
- managers of alternative investment funds;
- management companies;
- data reporting service providers;
- insurance and reinsurance undertakings;
- insurance intermediaries, reinsurance intermediaries, and ancillary insurance intermediaries;
- institutions for occupational retirement provision;
- credit rating agencies;
- administrators of critical benchmarks;
- crowdfunding service providers;
- securitisation repositories;
- ICT third-party service providers

03 | Who are the responsible regulators?

The lead overseers under DORA are specific supervisory authorities appointed to oversee critical ICT service providers that deliver essential digital services to financial institutions across the European Union.

These overseers are not national regulators but are appointed from one of the three European Supervisory Authorities (the European Banking Authority, the European Securities and Markets Authority, or the European Insurance and Occupational Pensions Authority). They act as the EU's top-level supervisors over the tech providers that underpin the digital infrastructure of the financial system.

The competent local regulatory authority in Hungary is the National Bank of Hungary ("NBH"), which is responsible for enforcing DORA at the national level.

04 | What are the key requirements?

DORA is structured around five key pillars:

I. ICT Risk Management – Businesses must implement robust cybersecurity measures to mitigate ICT-related risks. This includes conducting regular security testing, vulnerability assessments, and ensuring that senior management plays a central role in ICT risk governance, thereby integrating cybersecurity into the overall business strategy and decision-making processes.

II. Incident Reporting – Companies are required to promptly detect, classify, and report significant ICT-related incidents. These incidents must be reported using a standardised format, which will be developed by the European Supervisory Authorities, ensuring consistency across the industry and enabling a more effective and coordinated response to incidents.

III. Digital Operational Resilience Testing – Companies must conduct regular penetration testing, vulnerability assessments, and scenario-based exercises to evaluate their operational resilience. For critical financial institutions, Threat-Led Penetration Testing is mandatory at least every three years to assess vulnerabilities from the perspective of a cyber attacker, ensuring a more comprehensive security evaluation.

IV. ICT Third-Party Risk Management – DORA requires enhanced oversight of external ICT service providers, including the introduction of mandatory contractual obligations, regular compliance checks, and ensuring that third parties meet the necessary operational resilience standards. The European Supervisory Authorities will identify and designate certain ICT providers as critical, placing additional regulatory requirements on those entities to ensure the continuity and security of services.

V. Cyber Threat Intelligence Sharing – DORA promotes collaboration across the financial sector to strengthen cybersecurity defences by encouraging the sharing of cyber threat intelligence. This collaborative approach enables institutions to stay ahead of emerging cyber threats, improving overall resilience across the sector and reducing the likelihood of successful attacks.

05 | What steps and actions should be undertaken?

To ensure compliance with DORA, financial entities must adopt a strategic and integrated approach to enhancing their digital resilience capabilities.

1. Conduct a gap analysis – The first step involves conducting a comprehensive gap analysis to assess current ICT risk management practices against DORA's regulatory standards, identifying deficiencies and prioritising remedial actions based on operational and regulatory risk.

2. Strengthen governance structures – Governance frameworks should be reinforced by clearly assigning roles and responsibilities for ICT risk oversight at both the executive and board levels, embedding digital resilience within the broader enterprise risk management structure.

3. Strengthen third-party risk management – Entities must also revise their third-party risk management frameworks, ensuring that all ICT outsourcing contracts incorporate mandatory clauses on service availability, data protection, access rights, and termination. Continuous monitoring and auditing of third-party performance should be institutionalised.

4. Develop an incident reporting protocol – A robust incident management framework must be established, including defined classification criteria, escalation paths, and reporting protocols that align with the standardised formats prescribed by the European Supervisory Authorities.

Personnel should be trained in incident handling and simulated exercises conducted to test response readiness.

5. Implement regular cybersecurity testing – Cybersecurity testing should be embedded into the operational lifecycle, including periodic penetration tests, scenario-based exercises, and – where applicable – Threat-Led Penetration Testing for significant entities. The findings from these exercises must inform adaptive risk controls and system improvements.
6. Establish cyber intelligence sharing mechanisms – Organisations are also encouraged to engage in cyber threat intelligence sharing initiatives, enabling proactive threat detection and coordinated sectoral responses.
7. Educate employees and management – Finally, a strong emphasis must be placed on internal awareness, with tailored training programs for staff and management to foster a culture of security and regulatory compliance across the enterprise.

06 | What are the sanctions?

DORA does not set fixed EU-wide penalties. Instead, it requires each Member State to implement its own sanctions regime and empower its national regulators to enforce the rules. The focus is on ensuring compliance by financial institutions, with serious consequences for repeated or significant breaches.

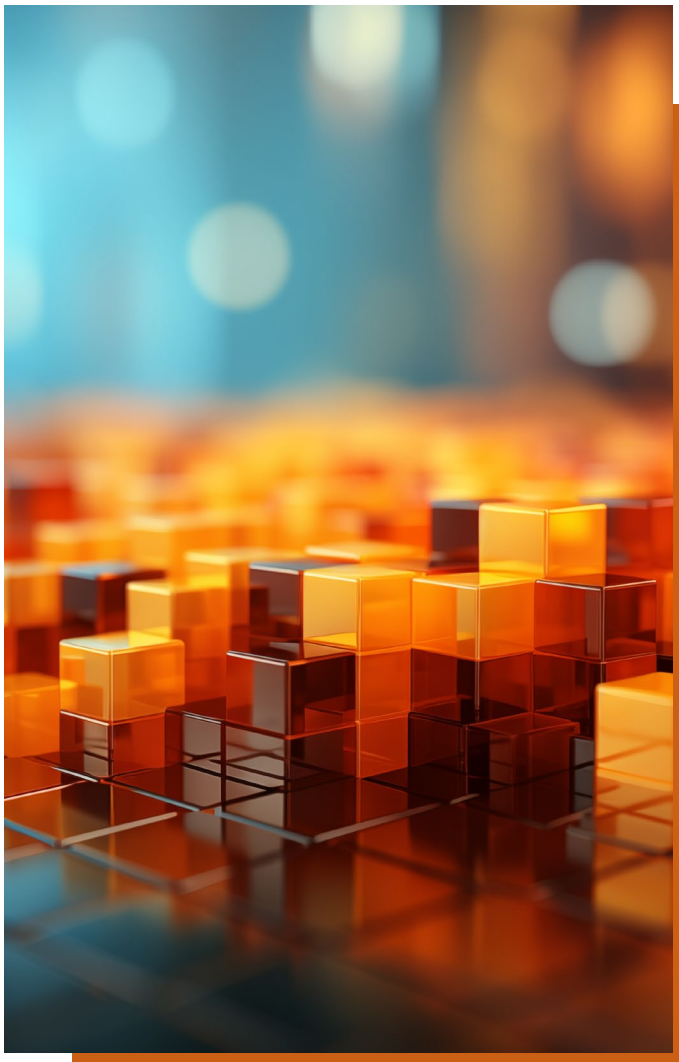
The National Bank of Hungary, which oversees the financial sector, ensures compliance with DORA and has the authority to impose a broad range of sanctions in the event of rule violations. These sanctions may include, but are not limited to, the following measures: (i) establishing the occurrence of the infringement; (ii) ordering the cessation of the infringement; (iii) prohibiting any further violations; (iv) imposing obligations necessary to terminate the infringement or mitigate its potential effects; and/or (v) levying a fine. With respect to critical ICT third-party service providers, DORA also sets out the range of sanctions that may be imposed by the lead overseers.

Levente Hegedűs
Partner

+36 1 428 4403
levente.hegedus@kinstellar.com

Dorottya Bitó
Associate

+36 1 428 4499
dorottya.bito@kinstellar.com



KAZAKHSTAN

01 | Main legislation regulating operational resilience for the financial sector

The main legal acts regulating the management of ICT risks in the financial sector in Kazakhstan include:

a. Law of the Republic of Kazakhstan dated 4 July 2003 No. 474-II "On State Regulation, Control and Supervision of Financial Market and Financial Organisations" (as amended);

b. Law of the Republic of Kazakhstan dated 24 November 2015 No. 418-V "On Informatisation" (as amended);

c. Law of the Republic of Kazakhstan dated 31 August 1995 No. 2444 "On Banks and Banking Activities in the Republic of Kazakhstan" ("**Bank Law**");

d. Secondary legislation of the Agency of the Republic of Kazakhstan on Regulation and Development of Financial Market (the "**Agency**") and the National Bank of the Republic of Kazakhstan ("**National Bank**").

02 | Who needs to comply?

Under the above-mentioned legislation, compliance is required by:

- financial organisations, which include inter alia: banks, branches of non-resident banks, insurance (reinsurance) organisations, other participants (brokers, dealers, investment portfolio managers); and
- ICT third-party service providers (cloud services, data analytics, etc.) – in relation to personal data protection.

03 | Who are the responsible regulators?

The responsibilities for oversight are distributed between the National Bank and the Agency.

04 | What are the key requirements?

- Key requirements for banks (Bank Law)

Banks must ensure backup systems for service continuity that help a bank quickly recover and continue operations if their main systems fail.

Clients must be notified about system updates affecting services.

An information security management system is required to protect the bank's data, systems, and customer information from cyber threats.

Security incidents must be reported to the regulator, critical incidents may be expedited to the National Cybersecurity Center.

- Cybersecurity in insurance (reinsurance) organisations

Insurance (reinsurance) organisations must ensure the confidentiality, integrity, and availability of data, including protection from unauthorised access. (Agency Management Board Resolution No. 164 dated 30 July 2018).

- Competence of informational security staff

Specific qualification and training requirements apply to informational security chiefs and cybersecurity departments (Agency Management Board Resolution No. 89 dated 21 September 2020).

- Mandatory Reporting of Cyber Incidents

Organisations must connect to the national cyber incident monitoring system and report all relevant security events (Resolution No. 76 dated 12 September 2022).

05 | What steps and actions should be undertaken?

1. Current challenges

- The primary risks include the rapid growth of online banking services, the advancement of remote work, the rise of digital fraud, and an increase in cyberattacks targeting financial organisations.
- As global cybersecurity standards continue to evolve, Kazakhstan faces the challenge of adapting its regulations and practices to meet these emerging risks.

2. What's been done

In partnership with the National Bank, the Agency developed a Cybersecurity Strategy for the Financial Sector (2020–2022), which focuses on addressing these challenges.

Key initiatives under this strategy include:

- the development of methodologies for assessing information security risks;
- updating security regulations for banks and the capital markets;
- establishing clear rules for incident response and the necessary competencies for staff working in financial organisations.

3. Additional measures that may be considered

- require comprehensive third-party risk management policies, especially for cloud and fintech vendors;
- conduct sector-wide cybersecurity drills simulating real incidents;
- expand the Agency's powers to supervise data protection and security compliance;

06 | What are the sanctions?

The Agency may impose limited measures of influence, measures of supervisory response, including with the use of motivated judgement, sanctions, and other measures provided by the laws of the Republic of Kazakhstan.

Additionally, Article 215-1 of the Code of Administrative Offences of the Republic of Kazakhstan No. 235-V dated 5 July 2014 (as amended) establishes fines for non-compliance with ICT security requirements in the banking sector.

This provision specifically applies to entities that fail to meet the established standards for ensuring the security of information systems and data in the financial services industry.

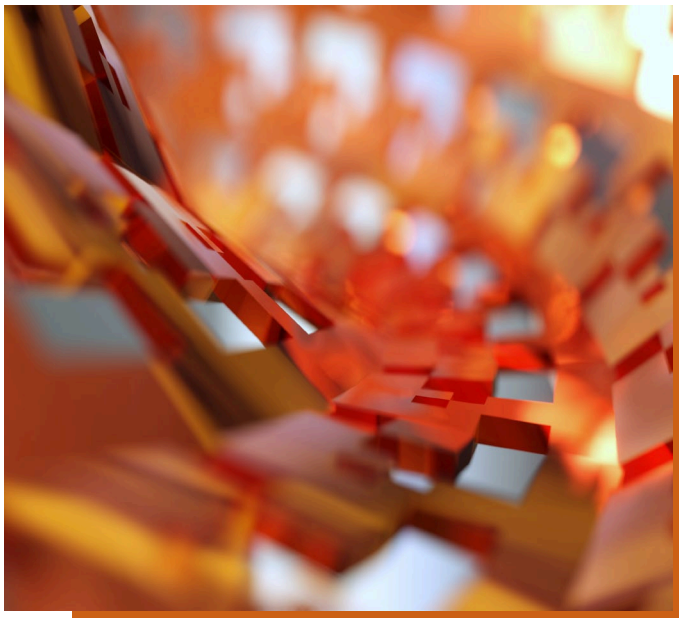
The law holds banks and financial organisations accountable for not adhering to cybersecurity regulations, and fines are imposed as a penalty for non-compliance.

Joel Benjamin
Managing Partner

+7 727 355 0530
joel.benjamin@kinstellar.com

Yerlan Akhmetov
Counsel

+7 727 355 0566
yerlan.akhmetov@kinstellar.com



ROMANIA

01 | Main legislation regulating operational resilience for the financial sector

The main legislation governing operational resilience for the financial sector is the EU's Digital Operational Resilience Act ("DORA"), established by Regulation 2022/2554/EU on digital operational resilience.

DORA is complemented by various implementing and delegated acts that provide further guidance and details on specific aspects of the Regulation. A full list of these implementing and delegated acts can be found here.

In addition to the EU legislation, national legislation has been adopted in Romania to implement DORA into Romanian law, namely:

- Emergency Ordinance No. 155/2024 on establishing a framework for cybersecurity of networks and information systems in national civil cyberspace;
- Law No 306/2024 amending and supplementing Law No 126/2018 on markets in financial instruments, amending and supplementing Government Emergency Ordinance No 32/2012 on undertakings for collective investment in transferable securities and investment management companies, amending and supplementing Law No 297/2004 on the capital market, and amending and supplementing Law No 74/2015 on alternative investment fund managers (in force since 17 January 2025);
- Law No.16/2025 amending and supplementing certain normative acts in the financial sector.

02 | Who needs to comply?

DORA applies to a wide range of financial entities, as well as certain ICT third-party service providers. Specifically, financial entities which need to comply include:

- banks and other credit institutions;
- insurance and reinsurance firms;
- investment firms;
- payment service providers;
- crypto-asset service providers.

In addition to those mentioned above, DORA also applies to critical third-party ICT service providers supplying cloud services, data analytics, and other essential services to financial institutions.

03 | Who are the responsible regulators?

The National Bank of Romania is the competent authority under DORA.

As the regulatory authority for the financial sector, the National Bank of Romania also cooperates with the Financial Supervisory Authority to ensure the compliance of financial institutions with the security requirements laid down in DORA.

04 | What are the key requirements?

DORA is structured around five key pillars:

I. ICT Risk Management – Companies must implement strong cybersecurity measures, conduct regular security testing, and involve senior management in ICT risk governance.

II. Incident Reporting – Companies must detect, classify, and report significant ICT-related incidents promptly using a standardised format. The European Supervisory Authorities will create a unified reporting format.

III. Digital Operational Resilience Testing – Companies must conduct regular penetration testing, vulnerability assessments, and scenario-based exercises. Critical financial firms must conduct Threat-Led Penetration Testing at least every three years.

IV. ICT Third-Party Risk Management – Enhanced oversight of external ICT service providers, including mandatory contractual obligations and compliance checks. The European Supervisory Authorities will designate certain ICT providers as critical.

V. Cyber Threat Intelligence Sharing – Encourages collaboration across the financial sector to improve cybersecurity defences.

05 | What steps and actions should be undertaken?

1. Conduct a gap analysis to assess current ICT risk management practices and identify areas for improvement.
2. Strengthen governance structures by assigning clear roles and responsibilities for ICT risk management.
3. Strengthen third-party risk management by reviewing vendor contracts and establishing mandatory security requirements.
4. Develop an incident reporting protocol aligned with DORA's reporting requirements to ensure timely and accurate reporting.
5. Implement regular cybersecurity testing, including penetration testing, scenario-based exercises, and operational resilience drills.
6. Establish cyber intelligence sharing mechanisms to collaborate with industry peers and regulators on emerging threats.
7. Educate employees and management on DORA's requirements and cybersecurity best practices to improve organisational awareness.

06 | What are the sanctions?

Financial entities and ICT third-party service providers may face significant sanctions for breaching obligations under DORA. The sanctions are set out in Emergency Ordinance No. 155/2024 on establishing a framework for cybersecurity networks and information systems in national civil cyberspace (the "Emergency Ordinance").

The Emergency Ordinance provides for administrative fines of up to:

- EUR 7,000,000 or 1.4% of net turnover, whichever is higher, for important entities, as defined by the Emergency Ordinance;
- EUR 10,000,000 or 2% of net turnover, whichever is higher, for essential entities, as defined by the Emergency Ordinance.

The fines listed above sanction more serious breaches, such as the failure to take technical, operational and organisational measures, to submit to a cybersecurity audit, to provide data required by the ordinance, or to undergo cybersecurity training.

In addition to fines, complementary measures such as the temporary suspension of certificates and authorisations, the publication of infringements, and temporary bans on the entity's management can be imposed.

Magdalena Raducanu
Partner

+40 21 307 1620
magdalena.raducanu@kinstellar.com

Razvan Constantinescu
Managing Associate

+40 21 307 1625
razvan.constantinescu@kinstellar.com

SERBIA

01 | Main legislation regulating operational resilience for the financial sector

Serbia has not yet aligned its legislation with the EU's Digital Operational Resilience Act ("DORA"). However, Serbia has a legal framework in place that establishes measures for the protection of information and communication systems, regulated under the Information Security Act (Zakon o informacionoj bezbednosti) ("Official Gazette of the RS", nos. 6/2016, 94/2017 and 77/2019). This Act regulates measures for the protection against security risks in information and communication systems, the responsibilities of legal entities in managing and using information and communication systems, and defines the competent authorities for implementing protective measures, coordinating between the protection entities, and monitoring the proper application of the prescribed protective measures. Furthermore, the Serbian government has published a new draft of the Information Security Act, which is expected to be adopted soon. The primary reason for adopting the new law is alignment with the NIS2 Directive.

Additionally, the National Bank of Serbia ("**NBS**") has enacted the Decision on minimum standards for the management of the information system of a financial institution (*Odluka o minimalnim standardima upravljanja informacionim sistemom finansijske institucije*) ("Official Gazette of the RS", nos. 23/2013, 113/2013, 2/2017, 88/2019, 37/2021 and 100/2023) ("Decision"), defining fundamental requirements for the management of information systems in financial institutions. As of 1 January 2026, the currently applicable Decision will be replaced by the Decision on minimum standards for the management of the information system of a financial institution (*Odluka o minimalnim standardima upravljanja informacionim sistemom finansijske institucije*) ("Official Gazette of the RS", no. 102/2024).

02 | Who needs to comply?

The Decision a broad spectrum of financial institutions:

- banks;
- insurance firms;
- financial leasing companies;
- voluntary pension fund management companies;
- payment institutions (i.e., payment services providers);
- electronic money institutions;
- the public postal operator.

03 | Who are the responsible regulators?

For the entities listed under point 2, the responsible regulator is the NBS.

04 | What are the key requirements?

The Decision defines the main requirements for financial institutions concerning information system management:

I. Establishment of an Adequate Information System – financial institutions are required to establish an adequate information system that fulfils requirements imposed by the law.

I. Internal Audit of the Information System – financial institutions are required to define criteria, methods, and procedures for the internal audit of the system in its internal audit methodology, based on the results of the risk assessment.

II. Information System Security Policy – financial institutions are obliged to enact an information system Security Policy, defining, inter alia, the internal organisation and division of duties and responsibilities among staff, appointment of key personnel, and their responsibilities and internal control.

III. Business Continuity Management and Disaster Recovery – financial institutions are required to establish a business continuity management process for the purpose of ensuring the uninterrupted and continuous functioning of all its critical systems and processes, as well as to limit losses in emergency situations.

IV. Development and Maintenance of the Information System – financial institutions are required to establish a process for the development of the information system in accordance with relevant changes within the financial institution and in the environment, in order to ensure the continuous adequacy of the system.

V. Electronic Services – if a financial institution provides electronic services, it is required to establish, as an integral part of information system risk management, a process for managing risks arising from the provision of electronic services.

05 | What steps and actions should be undertaken?

A financial institution should ensure that it duly meets all requirements set out in the Decision and regularly monitors compliance with applicable laws.

06 | What are the sanctions?

There is no single sanction system applicable to all financial institutions. The applicable sanctions depend on the type of financial institution.

Nevena Milošević
Senior Associate

+381 62 8809 312
nevena.milosevic@kinstellar.com

SLOVAKIA

01 | Main legislation regulating operational resilience for the financial sector

The main legislation governing operational resilience for the financial sector in the Slovak Republic is the EU's Digital Operational Resilience Act ('DORA"), established by Regulation 2022/2554/EU on digital operational resilience.

Slovak Act no. 747/2004 Coll. on Supervision over the Financial Sector has been adopted to implement DORA into national legislation.

02 | Who needs to comply?

- banks and other credit institutions;
- insurance and reinsurance firms;
- investment firms;
- payment service providers;
- crypto-asset service providers;
- ICT third-party service providers (cloud services, data analytics, etc.)

DORA also applies to critical third-party ICT providers that offer essential services to financial institutions.

03 | Who are the responsible regulators?

The National Bank of Slovakia (https://nbs.sk/en/) is empowered under national legislation to act as the regulator.

04 | What are the key requirements?

DORA is structured around five key pillars:

I. CT Risk Management – Companies must implement strong cybersecurity measures, conduct regular security testing, and involve senior management in ICT risk governance.

II. Incident Reporting – Companies must detect, classify, and report significant ICT-related incidents promptly using a standardised format. The European Supervisory Authorities will create a unified reporting format.

III. Digital Operational Resilience Testing – Companies must conduct regular penetration testing, vulnerability assessments, and scenario-based exercises. Critical financial firms must conduct Threat-Led Penetration Testing at least every three years.

IV. ICT Third-Party Risk Management – Enhanced oversight of external ICT service providers, including mandatory contractual obligations and compliance checks. The European Supervisory Authorities will designate certain ICT providers as critical.

V. Cyber Threat Intelligence Sharing – Encourages collaboration across the financial sector to improve cybersecurity defences.

05 | What steps and actions should be undertaken?

1. Conduct a gap analysis to assess current ICT risk management practices and identify areas for improvement.
2. Strengthen governance structures by assigning clear roles and responsibilities for ICT risk management.
3. Strengthen third-party risk management by reviewing vendor contracts and establishing mandatory security requirements.

4. Develop an incident reporting protocol aligned with DORA's reporting requirements to ensure timely and accurate reporting.
5. Implement regular cybersecurity testing, including penetration testing, scenario-based exercises, and operational resilience drills.
6. Establish cyber intelligence sharing mechanisms to collaborate with industry peers and regulators on emerging threats.
7. Educate employees and management on DORA's requirements and cybersecurity best practices to improve organisational awareness.

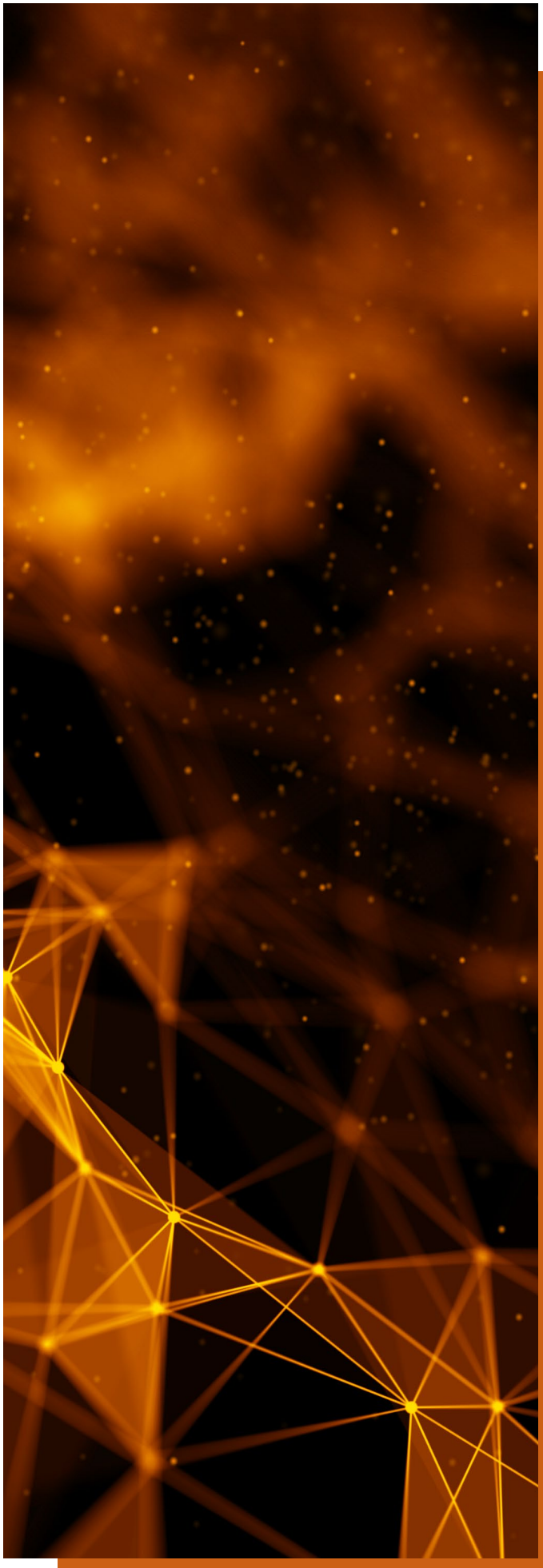
06 | What are the sanctions?

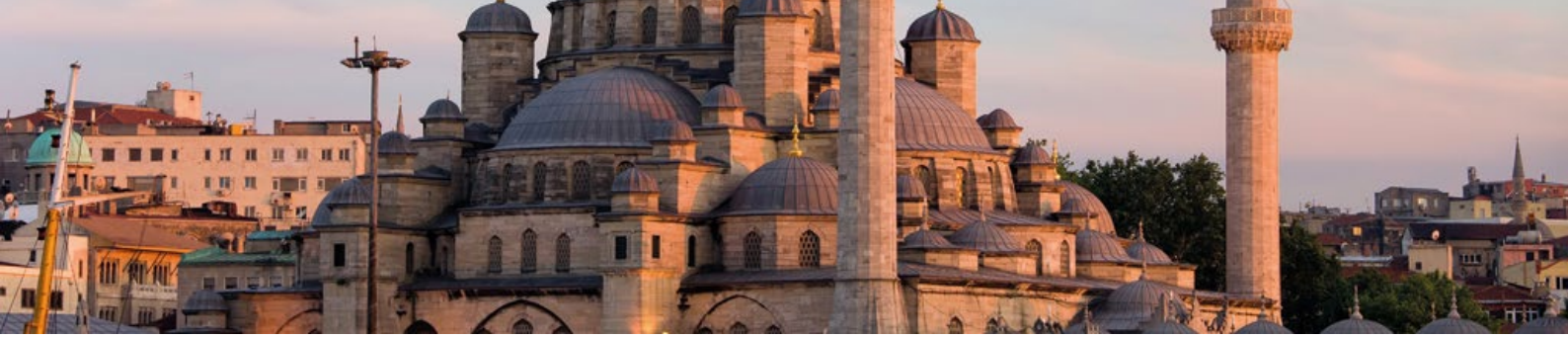
The National Bank of Slovakia may impose various administrative penalties and remedial measures including:

i. require the financial institution to adopt recovery measures and set a deadline for their implementation;
ii. impose fine in the amount of EUR 3,300 up to 10% of the total net annual turnover for the previous calendar year;
iii. require cessation of conduct which is in breach of DORA;
iv. suspend or withdraw the license; and
v. others.

Tomáš Melišek
Partner

+421 2 5929 1125
tomas.melisek@kinstellar.com





TURKEY

01 | Main legislation regulating operational resilience for the financial sector

The Turkish Banking Regulation and Supervision Agency ("**BRSA**") is the main regulator of the financial sector (with the exception of capital market-related actors, for which the Capital Markets Board is authorised). To the extent permitted by Turkish Banking Law, secondary legislation is issued by the BRSA. In this context, the BRSA has regulated the mandatory procedures and principles of risk management for the information systems used by banks in the performance of their activities. In Turkey, the BRSA has adopted the Regulation on Information Systems and Electronic Banking Services of Banks ("**Regulation**"), effective as of 1 July 2020.

02 | Who needs to comply?

Parallel to the authorities of the BRSA, banks need to comply with the Regulation.

03 | Who are the responsible regulators?

BRSA is the responsible regulator for the Regulation.

04 | What are the key requirements?

Key requirements and objectives of the Regulation are stipulated under six parts:

I. Information Systems Governance – addressing the management of information systems as part of corporate governance practices; preparing plans, procedures and process documents; establishing internal committees in this regard.

II. Managing Information Systems Risks – preparation of information assets inventory; establishment of risk management process with related action plans.

III. Information Security Management – conducting regular threat and risk assessments; taking appropriate security measures; monitoring and reporting security breach incidents.

IV. System Development and Change Management – ensuring the integrity and consistency of the data to be processed and stored through information systems; minimising data duplication; preparing the information architecture model.

V. Information Systems Continuity and Accessibility Management – maintaining primary and secondary systems in-country; establishing a help-desk function and a problem management system; implementing a performance monitoring process.

VI. External Service Procurement – due diligence in the selection of the service provider; monitoring the compliance of outsourcing processes with the Bank's processes; performing of internal control activities.

05 | What steps and actions should be undertaken?

1. Information security policies, procedures, and process documents must be prepared and reviewed at least once a year.
2. An information security officer should be appointed.
3. All data confidentiality measures must be taken.

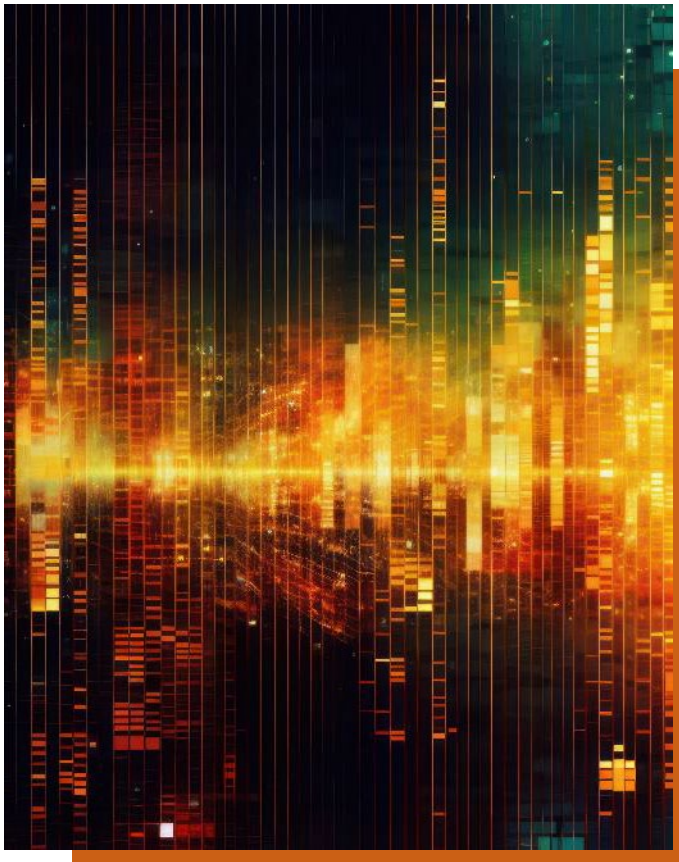
1. Information security policies, procedures, and process documents must be prepared and reviewed at least once a year.
2. An information security officer should be appointed.
3. All data confidentiality measures must be taken.
4. Access controls must be provided to persons with defined duties and responsibilities when accessing information assets.
5. An effective audit trail mechanism, network system, and security configuration information should be established for transactions and events occurring in information systems in proportion to the size and complexity of the systems and activities.
6. Banks should establish a cyber incident response process and report cyber incidents to the BRSA in order to return information systems to normal operation as soon as possible after a cyber incident with minimal impact on banking activities.
7. Banks should keep development, test, and production environments separate from each other in accordance with the principle of segregation of duties in the software development process.
8. Banks are required to keep their primary and secondary systems in-country.
9. An information systems continuity management process and plan should be prepared, a continuity management process officer should be appointed, and a continuity committee should be established to ensure the continuity of information systems services used in the conduct of banking activities.
10. An adequate oversight mechanism should be established to adequately assess and manage the risks posed to the bank by outsourced services and to ensure that relations with the outsourced service provider are carried out effectively.
11. Educate employees and management on the Regulation's requirements and best practices regarding information systems to improve organisational awareness.

06 | What are the sanctions?

BRSA is authorised to impose administrative fines against persons violating the secondary legislation, such as the Regulation.

Mert Elçin
Partner
mert.elcin@kinstellar.com

Helin Akbulut
Associate
helin.akbulut@ksthukuk.com



UKRAINE

01 | Main legislation regulating operational resilience for the financial sector

Although the EU's Digital Operational Resilience Act ("DORA") has not been implemented in Ukraine, there are national legislative acts aimed at enhancing the operational resilience of the financial sector.

The Law of Ukraine on the Basic Principles of Cybersecurity of Ukraine No 2163-VIII dated 5 October 2017 (the "**Cybersecurity Law**") is a key legislative act that defines the legal and organisational framework for ensuring the cybersecurity of the state, including the financial sector. Considering the EU legislation and the requirements of the Cybersecurity Law, the National Bank of Ukraine (the "**NBU**") has updated its approaches to risk management in the financial sector by adopting number of regulatory acts:

- Regulation "On Organisation of Risk Management Systems in Banks and Banking Groups of Ukraine", approved by Resolution of the NBU No. 64 dated 11 June 2018 ("**Regulation No. 64**"), defines the basic principles of risk management arising from the activities of a bank and a banking group at all organisational levels and establishes minimum requirements for organising a comprehensive and effective risk management system.
- Regulation "On the Organisation of Information Security Measures in the Banking System of Ukraine", approved by Resolution of the NBU No. 95 dated 28 September 2017 ("**Regulation No. 95**"), provides for mandatory minimal requirements for organising information security and cybersecurity measures, principles of information security management, and requirements for bank information systems that interface with the NBU's information systems, taking into account the development of cryptographic protection of information in the NBU's information systems.
- Regulation "On Monitoring Banks' Compliance with Legislative Requirements on Information Security, Cyber Security and Electronic Trust Services", approved by Resolution of the NBU No. 4 dated 16 January 2021("**Regulation No. 4**"), defines the procedure under which the NBU controls banks' compliance with legal requirements in the sectors of cyber defence and information security, as well as requirements for banks to conduct self-assessment of their information security/cyber defence.
- Regulation "On the Organisation of Cyber Defence in the Banking System of Ukraine", approved by Resolution of the NBU No. 178 dated 12 August 2022 ("**Regulation No. 178**"), establishes clear principles for the organisation and functioning of the cyber defence system in the banking sector
- Regulation "On Requirements to the Management System of Financial Payment Services Provider", approved by Resolution of the NBU No. 123 dated 10 October 2024 ("**Regulation No. 123**") sets requirements for the information security management system for non-banking financial institutions.

02 | Who needs to comply?

The NBU's regulations apply to banks and non-banking providers of financial payment services.

In addition, the NBU is currently developing a new Regulation on the organisation of measures to ensure information security and cyber security by financial service providers. Its requirements will apply to insurers, credit unions, financial companies, and pawnshops.

03 | Who are the responsible regulators?

In Ukraine, the primary regulatory authority responsible for overseeing ICT risk management and cybersecurity in the financial sector is the NBU. In particular, the Cyber Defence Centre of the NBU was established in 2017 to control cybersecurity and cyber defence activities in the banking and financial sectors.

04 | What are the key requirements?

I. IICT Risk Management

Banks and financial service providers are required to establish effective measures for managing ICT and information security risks, as well as maintaining a database of these risks and analysing the information gathered therein. There is also an obligation for banks to conduct an annual self-assessment of the state of information security/cybersecurity by preparing a Report.

II. Incident Reporting

The NBU establishes requirements for banks to report on significant cyber incidents. Payment service providers are obliged to ensure the development, documentation, and periodic updating of the payment service incident management policy, as well as measures related to the implementation of this policy. Detected cyber incidents or cyber crimes should be promptly reported to the NBU in electronic form or via postal mail in paper form.

III. Digital Operational Resilience Testing

Financial payment service providers must conduct operational risk stress testing at least once a year for various short-term and long-term stress scenarios that may occur both for the financial payment service provider and for the market as a whole in order to identify the causes of possible losses due to operational risk and to assess whether the results of stress testing comply with the established level of risk appetite for operational risk (not applicable to financial payment service providers that are classified as microfinance institutions).

IV. ICT Third-Party Risk Management

Currently, there is no specific legal framework in Ukraine that directly regulates the management of ICT third-party risks in the financial sector.

V. Cyber Threat Intelligence Sharing

The sharing of cyber threat intelligence is becoming increasingly important for enhancing resilience across the financial sector. While not explicitly outlined in Ukrainian regulations, the Cybersecurity Law encourages collaboration among public and private entities, including financial institutions, to share information on cyber threats. Additionally, Regulation No. 178 implies the importance of information exchange between banks and the NBU and the organisation of such a process.

05 | What steps and actions should be undertaken?

The NBU is considering additional regulations to extend cyber and information security requirements to a broader range of financial service providers, such as insurers, credit unions, etc. Once such regulation is adopted, financial service providers will need to ensure compliance and to manage ICT in accordance with the procedures established thereunder.

Furthermore, the NBU is in the process of strengthening the organisation of cyber protection for critical infrastructure objects of the Ukrainian banking system. The relevant provisions are included in the draft resolution of the NBU "On Critical Infrastructure of the Financial Sector", which was recently proposed for public discussion.

Considering the growing reliance on third-party ICT service providers, it is crucial to establish a clear framework to manage the risks associated with third-party suppliers. Financial institutions should implement comprehensive supervisory and governance mechanisms to manage such risks.

06 | What are the sanctions?

Pursuant to Article 12 of the Cybersecurity Law, anyone who violates cybersecurity legislation is subject to civil, administrative, or criminal liability.

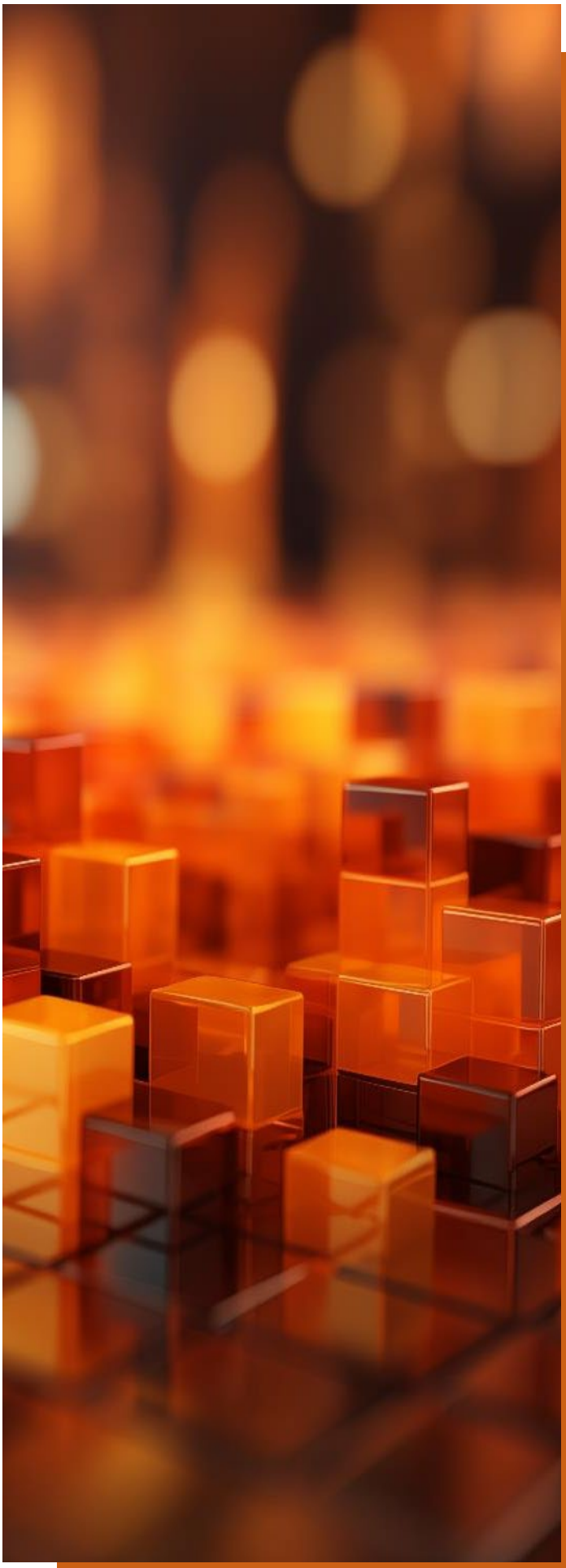
Moreover, Article 73 of the Law of Ukraine "On Banks and Banking Activities" provides the NBU with the authority to impose enforcement measures on banks and other entities that violate the requirements of cybersecurity and information security legislation. These measures may include written notification, imposing fines, or the limitation or suspension of certain operations, etc.

Illya Muchnyk
Partner

+380 44 490 9575
illya.muchnyk@kinstellar.com

Oleksandra Poliakova
Managing Associate

+380 44 490 9575
oleksandra.poliakova@kinstellar.com



UZBEKISTAN

01 | Main legislation regulating operational resilience for the financial sector

The primary legislation regulating operational resilience in the financial sector of Uzbekistan is derived from a combination of sector-specific laws, regulations issued by the Central Bank of the Republic of Uzbekistan ("CBU"), and broader legal frameworks that govern risk management and corporate governance.

The foundational legal act is the Law of the Republic of Uzbekistan "On the Central Bank of the Republic of Uzbekistan" No. 582 dated 11 November 2019 (the "Law on the Central Bank"), which vests the Central Bank with the authority to regulate and supervise the activities of commercial banks and other financial institutions, including requirements related to risk management, business continuity, and internal control systems. In particular, Article 9 of the Law on the Central Bank empowers the CBU to adopt normative acts aimed at maintaining financial stability and ensuring the reliability of the banking system.

Complementing the above is the Law "On Banks and Banking Activity" No. 580 dated 5 November 2019 (the "**Banking Law**"), which establishes the general obligations of banks to maintain robust internal control and risk management frameworks. Article 14 of the Banking Law specifically mandates that banks must implement internal policies aimed at managing all types of risks, including operational risk. The law further requires that risk management systems be integrated into the bank's decision-making processes and be subject to regular oversight by both executive management and supervisory boards.

At the regulatory level, the CBU has issued specific normative documents and guidelines that define standards for business continuity planning, IT and cybersecurity resilience, and operational risk management. These include:

- Regulation "[o]n the requirements for the system of banking and group banking risk management system", approved by the CBU Board (last updated in 2025), which outlines the expectations for operational resilience mechanisms, including identification, monitoring, and mitigation of operational risks.
- Regulation "[o]n protection of information in automated systems of commercial banks of the Republic of Uzbekistan", which incorporates principles aligned with international standards such as ISO/IEC 27033 and focuses on system integrity, data protection, and continuity of critical operations.

It is also important to note that the regulatory framework is gradually aligning with international standards such as the Basel Committee on Banking Supervision's Principles for Operational Resilience (2021), which, while not legally binding, are referenced in regulatory commentaries and are increasingly influencing local supervisory expectations.

Therefore, operational resilience in Uzbekistan's financial sector is not governed by a single comprehensive act, but rather by a layered system of legislation and regulations that collectively aim to ensure the continuity, reliability, and integrity of financial services, especially in the face of disruptions or systemic shocks.

02 | Who needs to comply?

In Uzbekistan, the obligation to comply with the regulatory framework on operational resilience primarily falls on a defined group of entities operating within the financial sector, as stipulated under various laws and regulations enforced by the CBU and other relevant supervisory authorities.

First and foremost, commercial banks are the key entities required to implement and maintain robust operational resilience measures. Under the Banking Law, all licensed banks must develop and operate internal control and risk management systems that address operational risks, including those related to IT systems, business continuity, and cyber threats.

Secondly, non-bank credit organisations, such as microcredit institutions and leasing companies that fall under the supervision of the CBU, are also subject to compliance requirements. While their regulatory burden may differ slightly in terms of scale and complexity, these entities are nonetheless required to maintain effective operational risk controls in line with the nature of their business.

Additionally, payment organisations and payment system operators, which are regulated under the Law "On Payments and Payment Systems" No. 578 dated 1 November 2019, are also mandated to ensure the security, reliability, and continuity of their services. Article 17 of this law outlines the requirements for ensuring the uninterrupted operation of payment systems, which inherently includes maintaining operational resilience against system failures or cyber incidents.

In the insurance sector, insurance companies and brokers must adhere to risk management obligations under the Law "On Insurance Activity" No. 730 dated 23 November 2021, although the specific regulatory instructions related to operational resilience are typically issued by the Insurance Market Development Agency.

Moreover, investment firms, securities market participants, and stock exchanges, regulated by the Capital Market Development Agency, are expected to manage operational risks, particularly those affecting the security of trading platforms and investor data.

Finally, outsourcing service providers that support critical operations of financial institutions, such as IT vendors or cloud service providers, while not directly regulated under banking laws, are indirectly bound by the compliance obligations imposed on the financial institutions they serve. Banks and other financial institutions are required to ensure that such third-party arrangements do not compromise operational resilience, as stipulated by CBU regulations and internal audit requirements.

In summary, compliance with operational resilience standards in Uzbekistan extends beyond just banks to include a broad spectrum of regulated financial institutions and, through them, certain critical service providers.

03 | Who are the responsible regulators?

The responsibility for regulating and enforcing operational resilience standards across Uzbekistan's financial sector is distributed among several supervisory authorities, each overseeing specific segments of the industry. These regulators not only issue binding requirements but also monitor compliance and impose corrective measures where necessary.

At the core of this regulatory framework is the CBU, which plays the principal role. As noted in the previous response, the CBU supervises all commercial banks, non-bank credit institutions, payment organisations, and payment system operators. Its authority is derived from the Law on the Central Bank and the Banking Law, which empower it to establish prudential standards, including those related to operational risk management, business continuity, and internal controls.

Through its regulatory instruments (e.g., regulations) the CBU sets expectations for the structure, documentation, testing, and audit of operational resilience frameworks. It also conducts on-site inspections and off-site monitoring to assess compliance and risk exposure.

In the insurance sector, responsibility lies with the Agency for Regulation and Development of the Insurance Market, which operates under the Ministry of Economy and Finance. This agency ensures that insurance companies and brokers implement adequate risk management systems, including the ability to withstand operational disruptions.

In some cases, there is also oversight from the CBU, State Tax Committee, and National Security Service, particularly when operational resilience intersects with anti-money laundering (AML) controls and data protection obligations.

Importantly, these regulators maintain an increasingly coordinated approach, especially as the Uzbek financial system moves toward greater integration with international standards. This is reflected in joint supervisory strategies, inter-agency memoranda, and the adoption of global frameworks such as the Basel III guidelines on operational risk and resilience.

Therefore, each category of financial institution—whether a commercial bank, payment system operator, insurer, or market intermediary—is subject to oversight by a specific regulator, but all operate within a harmonised structure designed to ensure the overall resilience and stability of the financial system.

04 | What are the key requirements?

The key requirements for operational resilience in Uzbekistan's financial sector are embedded in a framework of legal obligations and supervisory expectations aimed at ensuring that financial institutions can anticipate, withstand, and recover from disruptions—whether due to internal failures, cyber threats, or external shocks. These requirements are primarily defined by the CBU and are reinforced through specific sectoral laws and regulations.

At the core of these requirements is the establishment of comprehensive internal control and risk management systems. According to the Banking Law, particularly Article 42, all banks are obliged to identify, assess, monitor, and mitigate operational risks. The systems must be integrated into the institution's strategic planning and day-to-day operations, with oversight by both senior management and the supervisory board.

One of the central regulatory documents, the CBU's Regulation "On the requirements for the system of banking and group banking risk management system", sets out detailed criteria, including:

- Operational Risk Identification and Assessment: Institutions must establish procedures to identify and assess risks related to processes, systems, personnel, and external events that could disrupt normal operations. This includes risks related to IT systems, outsourcing, and cybersecurity threats.
- Business Continuity and Recovery Planning: Institutions are required to implement and regularly update business continuity plans and disaster recovery plans. These plans must outline the institution's strategy for maintaining critical operations in the event of disruptions and must be tested periodically to ensure effectiveness.
- IT and Cybersecurity Resilience: As set out in the Regulation "On protection of information in automated systems of commercial banks of the Republic of Uzbekistan", banks must implement secure IT infrastructure, regularly perform system vulnerability assessments, and ensure that data confidentiality, integrity, and availability are preserved. This includes having dedicated IT security policies and incident response procedures aligned with international standards.
- Governance and Accountability: The board of directors and executive management are directly responsible for the oversight of operational resilience. The law requires clear assignment of roles, with internal audit and compliance functions obliged to evaluate the adequacy of resilience measures independently.
- Reporting and Disclosure: Financial institutions must submit regular reports to the CBU detailing their risk exposures, incident history, and resilience strategies. This allows the regulator to assess systemic vulnerabilities and enforce remedial actions where necessary.
- Third-Party Risk Management: Given the increasing use of outsourcing and fintech solutions, banks must evaluate and monitor operational risks related to third-party service providers. Contracts must include clauses that ensure continuity of services and access to data in the event of provider failure.

While the precise scope of these requirements varies depending on the size and complexity of the institution, the regulatory expectation is that all financial institutions develop a proportionate and risk-based approach to operational resilience.

This ensures that even smaller institutions are adequately prepared to respond to events that may impact customer service, financial stability, or data integrity.

In summary, the operational resilience framework in Uzbekistan mandates a preventive, responsive, and forward-looking approach to risk management, integrating governance, IT security, continuity planning, and regulatory compliance into a cohesive strategy.

05 | What steps and actions should be undertaken?

To meet the operational resilience requirements in Uzbekistan's financial sector, institutions must take a structured and proactive approach, integrating legal obligations with best practices. These steps and actions are not only regulatory expectations—primarily under the supervision of the CBU—but also critical to safeguarding the continuity and integrity of financial services.

The process begins with a comprehensive risk assessment. Financial institutions must conduct a detailed analysis to identify critical business functions, interdependencies, and potential threats. This includes evaluating internal vulnerabilities (such as outdated IT systems or insufficient staff training) and external risks (such as cyberattacks, geopolitical instability, or natural disasters). The risk assessment forms the foundation for a tailored operational resilience strategy.

Following the assessment, institutions are required to develop and maintain robust internal policies and procedures. These should cover the management of operational risks, business continuity, IT security, incident response, and third-party risk. The internal documentation must clearly define roles and responsibilities, escalation paths, and key performance indicators for resilience-related processes. The CBU's normative guidance expects these policies to be approved by the board and periodically reviewed.

A critical next step is the implementation of Business Continuity Plans and Disaster Recovery Plans. These documents must specify how the institution will maintain or restore critical functions in the event of a disruption. The CBU requires that these plans be tested regularly—through simulations or real-time drills—and that lessons learned be integrated into plan revisions. For institutions operating digital services, the recovery time objectives and recovery point objectives must be clearly defined and achievable.

Strengthening IT and cybersecurity infrastructure is another essential area. Financial institutions must invest in secure architecture, regular patching, access control, and intrusion detection systems. As prescribed in the CBU's regulations, institutions must appoint a Chief Information Security Officer or equivalent function responsible for maintaining compliance with cybersecurity standards. They must also adopt internationally recognised frameworks such as ISO/IEC 27033, where applicable.

Training and awareness-building is equally important. All staff, from top management to operational personnel, should be trained on resilience protocols. In particular, employees must understand their roles in emergency scenarios and be familiar with internal communication channels and decision-making procedures.

Additionally, institutions must establish a framework for continuous monitoring and internal audit of their operational resilience posture. This includes the regular evaluation of risk controls, incident tracking, root cause analysis, and submission of reports to the CBU. The internal audit function plays a key role here, by independently reviewing the effectiveness of implemented measures and advising on improvements.

Finally, institutions must manage third-party and outsourcing risks with formal agreements that address continuity, data security, and regulatory access. The CBU expects that institutions retain ultimate responsibility for outsourced functions and must be capable of transferring or insourcing operations if a service provider fails.

To summarise, financial institutions in Uzbekistan must undertake a cycle of risk identification, policy implementation, resilience planning, testing, monitoring, and continuous improvement. These actions are not one-off requirements, but part of a dynamic and evolving strategy aligned with both national regulations and global best practices.

06 | What are the sanctions?

In Uzbekistan, the sanctions for non-compliance with operational resilience requirements in the financial sector are defined through a combination of regulatory enforcement mechanisms and legal provisions embedded in financial legislation. These sanctions are imposed primarily by the CBU and vary depending on the severity, duration, and systemic impact of the breach.

Under the Law on the Central Bank, particularly Article 67, the CBU holds the authority to conduct supervisory reviews and enforce corrective actions when institutions fail to meet their obligations, including those related to internal controls, operational risk management, and business continuity. If deficiencies are found—such as the absence of a functioning risk management system, failure to test business continuity plans, or inadequate cyber defences—the CBU can issue a prescription (in Russian: predpisaniye) requiring the institution to rectify the issue within a set timeframe.

If the institution fails to comply with the prescription or if the breach is deemed serious or systemic, the CBU may escalate sanctions, which can include:

- Imposition of fines: While specific amounts depend on the type of institution and violation, fines are typically based on the relevant provisions of the Banking Law. Articles 53–59 of this Code allows for penalties on legal entities and their officials for violations of banking and financial regulations, including improper risk management or failure to ensure operational security.
- Restriction or suspension of certain operations: The CBU has the right to temporarily restrict a bank or financial institution from performing specific operations, especially if continued operations could pose systemic risk or harm to consumers.
- Revocation or suspension of licenses: In cases of repeated or particularly egregious violations, the CBU may revoke the institution's license to operate.

In addition to regulatory sanctions, institutions that suffer operational failures resulting in harm to customers—such as loss of access to funds, data breaches, or service outages—may face civil liability under the general provisions of the Civil Code of Uzbekistan. They could be required to compensate for damages, particularly if gross negligence or inadequate planning can be demonstrated.

Furthermore, in cases involving data breaches, cybercrime, or money laundering facilitated by operational weaknesses, institutions and their responsible officials may face criminal liability under the Criminal Code, especially under articles related to negligence, abuse of power, or facilitation of illicit activities.

In summary, the Uzbek regulatory framework provides a full spectrum of sanctions for non-compliance with operational resilience requirements—from administrative measures and fines to license revocation and criminal prosecution. The CBU enforces these rules actively as part of its broader mandate to ensure financial stability, institutional integrity, and consumer protection.

Kamilla Khamraeva
Counsel

+998 93 386 3032
kamilla.khamraeva@kinstellar.com

Leading independent law firm in Central and Southeastern Europe and Central Asia

With offices in 12 jurisdictions and over 300 local and international lawyers, we deliver consistent, joined-up legal advice and assistance across diverse regional markets – together with the know-how and experience to champion your interests while minimising exposure to risk.

ALMATY, ASTANA | KAZAKHSTAN
BELGRADE | SERBIA
BRATISLAVA | SLOVAKIA
BUCHAREST | ROMANIA
BUDAPEST | HUNGARY
ISTANBUL | TURKEY
KYIV | UKRAINE
PRAGUE | CZECH REPUBLIC
SOFIA | BULGARIA
TASHKENT | UZBEKISTAN
VIENNA | AUSTRIA
ZAGREB | CROATIA

KINSTELLAR