BANKA QENDRORE E REPUBLIKËS SË KOSOVËS
CENTRALNA BANKA REPUBLIKE KOSOVO
CENTRAL BANK OF THE REPUBLIC OF KOSOVO

REGULATION ON INFORMATION SYSTEMS AND CYBER RISK MANAGEMENT

Contents

Based on Article 35, paragraph 1, subparagraph 1.1 and Article 65, paragraphs 1 and 2 of Law no. 03/L-209 on the Central Bank of the Republic of Kosovo (Official Gazette of the Republic of Kosovo, No. 77/16 August 2010), amended and supplemented by Law No. 05/L-150 (Official Gazette No. 10/03 April 2017), Article 85 and 114 of Law No. 04/L-093 on Banks, Microfinance Institutions and Non-Banking Financial Institutions (Official Gazette/No. 11/11 May 2012), Article 8 of Law No. 04/L-155, on the Payment System (Official Gazette/No. 12, 03 May 2013), Article 4, paragraph 3 of Law No. 05/L-045 on Insurance (Official Gazette No. 38/4 December 2015), Article 29 paragraph 8 of Law No. 04/L-018 on Compulsory Motor Liability Insurance (Official Gazette No. 4/11 July 2011), Article 4 paragraph 1, Article 20 paragraph 1, Article 13, paragraph 13.1, subparagraph (d) of Law No. 04/L-101 on Pension Funds of Kosovo (Official Gazette/ No. 10/8 May 2012) and Article 34 of Law No. 08/L-295 on Crypto-Assets (Official Gazette No. 21/22 November 2024), the Board of the Central Bank of the Republic of Kosovo, at its meeting held on 29 August 2025, approved the following:

REGULATION ON INFORMATION SYSTEMS AND CYBER RISK MANAGEMENT

CHAPTER I
GENERAL PROVISIONS

Article 1
Purpose and scope

1. This Regulation sets out the minimum standards, criteria and procedures for information technology and cyber risk for Financial Institutions (FIs) applied, depending on the complexity and level of use of information technology.
2. This Regulation applies to all Financial Institutions - licensed or supervised FIs by the Central Bank of the Republic of Kosovo (CBK).
3. This regulation does not apply to Non-Banking Financial Institutions that only carry out Foreign Exchange activities, as well as Insurance Intermediaries.

Article 2
Definitions

1. The terms and definitions used in this regulation have the following meanings:
   1.1. **Risk appetite**- The overall level and types of risk that an FI is willing to assume, established in advance and within its risk capacity, to achieve its strategic objectives and business plan.
   1.2. **Configuration Item (CI)**- A managed component of an IT system (hardware, software or documentation) followed for change management and service delivery.
   1.3. **Supporting assets**- People, technology, information and equipment necessary to carry out critical operations.

1.4. **Multi-Factor Authentication (MFA)** - A security mechanism that requires multiple forms of verification (e.g., passwords, biometrics, security tokens, etc.) before access is granted.

1.5. **Change Advisory Board (CAB)**- is a structure within the IT Change Management process that is tasked with reviewing, evaluating, and approving or rejecting proposals for changes in the IT environment.

1.6. **Board of Directors (BD)**- The governing body, responsible for overseeing the ICT risk management, operational sustainability, cybersecurity policies and compliance with regulatory requirements of an FI.

1.7. **Cloud Computing**- Use of scalable computing resources on demand, such as: data storage space, processing power and software - provided via the Internet.

1.8. **DevSecOps**- Integrating security practices into software development and IT operations, to ensure secure development of IT systems.

1.9. **Data encryption**- The process of encoding data to prevent unauthorized access, ensuring confidentiality and integrity.

1.10. **Incident** - any unplanned, unforeseen or intentional event that negatively affects or has the potential to negatively affect the confidentiality, integrity, availability or authenticity of data, information and communication technology (ICT) systems and services that support the critical or regulated functions of the FI, causing operational disruption, data loss, financial damage, risk to financial market stability or damage to the credibility and reputation of the institution. It is an event that has, or could potentially have, a negative impact on the confidentiality, integrity or availability of information or information systems of the FI

1.11. **Financial Institutions (FI)** – In the light of this Regulation, we will refer to Financial Institutions, or FI institutions, which include Banks, Microfinance Institutions, Non-bank Financial Institutions, Insurance Companies, Kosovo Insurance Bureau, Pension Savings Funds, Cryptocurrency Operators and other entities that carry out financial activities, as defined in any relevant Law for the purposes of this Regulation.

1.12. **Cyber Threat Intelligence (CTI)** - Collecting, analysing, and sharing information on cybersecurity threats to improve risk detection and mitigation.

1.13. **Data classification**- The process of categorizing data, based on the relevant legislation in force, depending on the level of sensitivity of compliance requirements and security needs.

1.14. **Risk Management Framework (RMF)**- A structured approach to defining roles, responsibilities, risk assessments, mitigating measures and monitoring activities related to ICT and cybersecurity.

1.15. **Never Alone**- A security principle that requires that critical or sensitive operations be performed in the presence of a larger number of authorized persons to prevent fraud or errors.

1.16. **Patch Management (Patch)**- A policy that governs the deployment of software patches to address security vulnerabilities and maintain system integrity.

1.17. **Safe Disposal Management** - Procedures that ensure the secure disposal of IT assets and data, while maintaining data privacy and environmental compliance.

1.18. **Identity Access Management (IAM)**- A framework that ensures secure and controlled access to IT systems, implementing principles such as: least privilege access, segregation of duties, and role-based access controls.

1.19. **Incident Management**- A systematic approach to detecting, responding to, mitigating and recovering from cybersecurity and ICT incidents.

1.20. **Outsourcing and Technology Service Provider Management – (OTSPM) -** Regulatory framework governing the use of external service providers for critical functions, ensuring accountability and compliance.

1.21. **Change Management**- A structured process that ensures that changes to ICT systems are assessed, approved, implemented and documented with minimal disruption.

1.22. **Technology Risk Management – (TRM)** - A structured approach to identifying, assessing, mitigating and monitoring risks related to ICT and cybersecurity.

1.23. **Artificial Intelligence (AI) Model Risk Management -** The process of ensuring that artificial intelligence models are transparent, explainable, auditable, and free from bias.

1.24. **ICT Risk Management**- The process of managing risks related to information and communication technology, ensuring secure and resilient operations.

1.25. **Security Management of Virtualized Systems** - Security measures for virtualized environments, including: hypervisors, virtual machines, and cloud-based infrastructure.

1.26. **Secure Data Center Management**- Measures that ensure the physical and cyber protection of an FI data center infrastructure.

1.27. **Secure Network Management**- Policies and controls that ensure the secure operation and segmentation of an FI's IT network.

1.28. **Business Continuity Management (BCM) -** A strategic approach to ensuring that critical business functions can continue during and after disruptions, whether as a result of cyberattacks, technical problems, or natural disasters.

1.29. **Risk Monitoring and Reporting**-Continuous assessment and reporting of Risk exposure to senior management and regulatory authorities.

1.30. **Segregation of Duties (SoD)**- A control mechanism that ensures that key responsibilities are shared among multiple individuals, to reduce the risk of fraud, errors or unauthorized actions.

1.31. **Application Programming Interfaces (API**) - Interfaces that enable systems to communicate securely, with controls that ensure confidentiality and data integrity.

1.32. **Need-to-Use Basis** – A restriction policy where access to systems, data, or resources is granted only when expressly required for a specific task or function.

1.33. **Technology Service Provider (TSP)** - An external entity that provides IT services, infrastructure, or applications to organizations, often under a contractual agreement.

1.34. **Third Party Service Providers** - External entities that provide ICT-related services, including cloud computing, outsourcing and cybersecurity solutions.

1.35. **Critical Operations** - The interruption of which would affect the continued operation of the FI or its role in the financial system. Whether a particular operation is "critical" depends on the nature of the FI and its role in the financial system.

1.36. **AI Regulatory Compliance** - Requirement for FIs to ensure that AI applications in critical functions meet legal and regulatory standards.

1.37. **Data Leak Prevention (DLP)** - Security measures and technologies designed to detect, monitor and prevent unauthorized access, transmission or modification of sensitive data.

1.38. **Phishing** -The deceptive practice of sending emails or other messages that claim to come from someone else, with the intent of tricking individuals into revealing their credentials or personal information, such as passwords, credit card numbers, or other confidential information.

1.39. **Cyber Incident Response Plan**- A set of predefined actions that a financial intermediary follows to contain, mitigate, and recover from a cyber-incident.

1.40. **Disaster Recovery Plan (DRP)** - A documented strategy for restoring ICT systems and data after a major failure or cyber incident.

1.41. **Secure Coding Practices**- Programming methodologies designed to prevent vulnerabilities, such as: injection attacks, data breaches, and system exploits.

1.42. **The Least Privilege**- A security principle where users, applications, or systems are granted only the minimum level of access necessary to perform their job functions.

1.43. **Cyber Security Operations Center (SOC)**- A centralized unit responsible for monitoring, detecting, analyzing, and responding to cybersecurity threats.

1.44. **Governance and Supervision**- The internal framework within a financial institution to manage Information and Communication Technology (ICT) and cyber risks prudently and effectively.

1.45. **Governance of Cloud Computing**- Overseeing Cloud-based services to ensure data security, regulatory compliance, and operational sustainability.

1.46. **Artificial Intelligence (AI) Governance**- Policies and frameworks that ensure ethical, responsible and regulatory compliant use of AI in financial services.

1.47. **Operational Sustainability**- It is the ability of an FI to conduct critical operations across operational constraints. This capability enables an FI to identify and protect against threats and potential failures, to respond and adapt, and to recover from and learn from disruptive events in order to minimize their impact on the conduct of critical operations across operational constraints. In considering its operational resilience, an FI should assume that disruptions will occur and take into account its overall risk appetite and tolerance for disruptions.

1.48. **Ransomware** - a type of malicious software that encrypts or locks the data and systems of a user or institution, demanding payment (ransom) to restore them to their normal state.

1.49. **Regulatory Reporting of Cyber Incidents**- Requirement for FIs to report cybersecurity incidents to the Central Bank of the Republic of Kosovo (CBK) within specified time frames.

1.50. **Redundant**– having additional or duplicate systems, components, or resources to provide backup in case the primary one fails — ensuring continuous operation and high availability.

1.51. **Conservation and Recovery**- The process of securely storing copies of data and ensuring their recovery in the event of damage or loss.

1.52. **End Device Security**- Measures to protect devices such as: workstations, laptops and mobile devices from cyber threats.

1.53. **Independent Audit Assurance** - Independent review process of ICT security controls, governance and regulatory compliance.

1.54. **Bring Your Own Device (BYOD)** - A policy that allows employees to use their personal devices, such as smartphones and laptops, for work purposes, offering flexibility and convenience but requiring careful management of security risks.

1.55. **Vulnerability scanning**- Regular assessments of ICT systems to identify and mitigate security vulnerabilities.

1.56. **ICT Strategy**- A plan that aligns ICT capabilities with the overall business objectives of the FI, covering systems advancements, cybersecurity policies, and third-party dependencies.

1.57. **Stress Test in AI**- The process of evaluating AI systems under different conditions to assess their stability and reliability.

1.58. **Distributed Denial of Service Attack (DDoS)**- A distributed denial of service (DDoS) attack is a cyber-attack that overloads a targeted system, network, or website with excessive traffic from multiple sources, causing slowdowns or outages.

1.59. **Penetration Testing**- Simulated cyber-attacks conducted to assess the protection and resilience of a financial institution's cybersecurity.

1.60. **Risk Management**- Implementing measures to mitigate or reduce risks to an acceptable level.

1.61. **Transparency of AI Decisions**- Requirement for FIs to disclose when decisions driven by artificial intelligence affect clients and to provide a complaints mechanism.

1.62. **Incident Response Exercises**- Testing and training activities to assess the effectiveness of an FI incident response plan.

1.63. **Virtualization**- the use of software technologies or techniques to create a layer of abstraction over physical information technology resources (servers, networks, data storage or desktops), in order to enable the separation, isolation and execution of independent logical environments on the same physical infrastructure.

1.64. **Supplier Competence Assessment**- Assessing third parties to ensure they meet the required expertise for contracted ICT functions.

1.65. **Risk assessment** - Identifying and assessing threats, vulnerabilities and potential consequences to determine the likelihood and impact of the risk.

1.66. **Threat and Vulnerability Risk Assessment (TVRA) -** A process that assesses potential threats and vulnerabilities in an organization's IT and physical environments, to determine security risks and mitigation strategies for identified risks.

1.67. **Chief Information Security Officer (CISO) -** A senior executive responsible for creating and maintaining an FI security vision, strategy and programs to protect information assets and ICT systems.

1.68. **Chief Technology Officer (CTO)** - An executive responsible for overseeing the technology strategy, infrastructure, and digital sustainability of an FI.

Article 3
Principle of Proportionality

1. All banks must comply with the requirements under the provisions of this regulation.
2. In addition to the institutions referred to in paragraph 1 of this Article, other institutions subject to this Regulation are responsible for ensuring compliance with the relevant requirements based on their size, overall risk profile, internal organization and the nature, scope, complexity and riskiness of their services, activities and operations, regardless of whether they are currently provided or intended.
3. In supervising financial institutions, the CBK will assess compliance with both the text and the spirit and purpose of this regulation, and its decisions on such matters are final. This principle of proportionality ensures that regulatory obligations are appropriately tailored to the specific characteristics and risks of each institution, while maintaining accountability for compliance.
4. FIs that have a higher level of complexity and technology in use may implement additional appropriate measures, including the use of advanced technologies, to mitigate such risks.

CHAPTER II
GOVERNANCE AND SUPERVISION

Article 4
Governance and organization

1. The FI must have a governance and internal control framework that ensures effective and prudent management of Information and Communication Technology (ICT) and cyber risks, with the aim of achieving a high level of digital operational sustainability.
2. The Board of Directors (BD) should review and approve the FI’s operational resilience approach, taking into account the FI’s overall tolerance for disruptions to its critical operations. In formulating the FI’s disruption tolerance, the BD should consider the FI’s operational capabilities, considering a wide range of severe but plausible scenarios that would impact its

critical operations. The BD should ensure that the FI's policies effectively address cases where the FI's capabilities are insufficient to meet the stated disruption tolerance.

3. The Board is responsible for approving all policies related to information systems (including, but not limited to, ICT, Information Security and/or Cyber) and must annually assess the adequacy of the policies and review them.
4. The FI's Board of Directors and senior management must ensure that effective internal controls and risk management practices are implemented to achieve the security and reliability of its ICT operating environment.
5. The BD and senior management should have members with the necessary experience to understand and manage technological risks, which include the risks posed by cyber threats.
6. The FI must have appropriate functions related to ICT management, ICT risk, ICT system security and business continuity.
7. The FI must designate a person or unit responsible for information security, who must manage the security of the information system and coordinate the information security policies and processes related to the functions and technological platforms. The unit or person responsible for information security must report to the Chief Executive Officer and must be independent of other organizational units. Through the Chief Executive Officer, it must report at least once a year and as needed to the Board of Directors, which must be informed of the operations and functions related to information security.
8. The FI shall appoint a Chief Information and Technology Officer and a Chief Information Security Officer, who possess the necessary expertise and experience. The CBK shall be informed 30 days in advance of such appointments, providing a justification for the proposed candidates. The CBK reserves the right to object to any such appointment during the notice period or at a later stage. The FI that, under Article 3 of this Regulation, decides not to appoint such roles shall ensure sufficient expertise, experience and independence to exercise such roles effectively.
9. The FI should ensure a sufficient number of FI staff with relevant skills to support their ICT operational needs and their ICT risk management processes, as well as to ensure the implementation of their ICT strategy, by allocating the necessary funds and providing appropriate training on ICT risks to staff members, including key function holders, on an annual basis or more frequently if necessary.
10. The BD and senior management should ensure that key ICT decisions are made in line with the FI's risk tolerance.
11. The BD and senior management should cultivate a strong culture of technological risk awareness and management, including cyber hygiene at all levels of FI staff.
12. The BD or a committee delegated within is responsible for:

    12.1. ensuring a sound and robust risk management framework;

    12.2. effectively implementing and maintaining policies, procedures and standards to manage ICT and cyber risks;

12.3. providing a Technology Risk Management (TRM) function to oversee the Technology Risk Management Framework And Strategy (TRMF), providing an independent perspective on the technological risks faced by the FI;

12.4. providing senior managers, who are responsible for the execution of the FI's TRMF, with sufficient authority, resources and access to the Board;

12.5. adopting a risk tolerance statement that articulates the nature and extent of technological risks that the FI is willing and able to assume;

12.6. regular review of the TRMF for continued relevance;

12.7. assessing management competencies for managing technological risks, and

12.8. ensuring the establishment of an independent audit function to assess the effectiveness of the FI's internal control environment, risk management and governance.

13. Senior management is responsible for:

13.1. the creation of the TRMF;

13.2. management of technological risks in accordance with the defined TRMF;

13.3. clearly defining the roles and responsibilities of staff in managing technological risks, and

13.4. immediately informing the Board of Directors of significant and adverse developments and incidents of technological risks that are likely to have a major impact on the IF.

Article 5
Strategy, policies and procedures

1. For proper management of Information and Communication Technology (ICT), the FI must:

1.1. Adopt an ICT strategy

1.2. Define action plans that support the implementation of the ICT strategy, and

1.3. Create processes to monitor and measure the effectiveness of the strategy.

2. The management body has overall responsibility for defining, approving and overseeing the implementation of the FI's ICT strategy as part of their overall business strategy, as well as for establishing an effective Risk Management framework for ICT and security risks to ensure compliance with applicable legislation/regulations.

3. The FI should align the ICT strategy with the overall business strategy, in order to cover:

3.1. How should ICT evolve to effectively support and implement the business strategy, including the evolution of the organizational structure, changes to the ICT system, and key dependencies with third parties;

3.2. The planned strategy and evolution of the ICT architecture, including dependencies on third parties; and

3.3. Clear information security objectives, focusing on ICT systems and ICT services, staff and processes.

4. In the action plan mentioned in paragraph 1, subparagraph 1.2 of this article, the FI determines the activities to be undertaken to achieve the objectives of the ICT strategy. The FI regularly reviews the action plans to ensure their relevance and appropriateness.

5. The FI should establish policies, standards and procedures, and, where appropriate, incorporate industry standards and best practices to manage technological risks and protect information assets. Policies, standards and procedures should also be reviewed and updated regularly (at least annually), taking into account the evolving technology and cyber threat environment.

6. ICT management policies should define at least the following elements:

   6.1. Administration and operation of ICT systems

   6.2. Organizational structure for ICT management

   6.3. Hardware and software infrastructure of the ICT field (configuration diagrams)

   6.4. Classification of documentation and protection of systems and data

   6.5. Backup of information systems data

   6.6. Business continuity plan

   6.7. Change management systems

   6.8. Incident management

   6.9. IT system Risk Management

   6.10. Defining security mechanisms for ICT systems, and

   6.11. Third party management.

7. Procedures should define specific steps and actions for the effective implementation of policies. They should ensure consistent, secure and efficient operations across all ICT systems. Each procedural element should be consistent with the defined policy areas, covering day-to-day operations, emergency response and methods to protect data integrity and system security.

8. The FI should fully review and assess the risks associated with deviations from approved policies, standards and procedures and obtain senior management approval for material deviations. Approved deviations should be reviewed periodically to ensure that residual risks are at an acceptable level.

9. Compliance processes (e.g., the three-line model) should be implemented to verify that policies, standards, and procedures are being followed. These include follow-up processes for non-compliance.

Article 6
ICT asset and information management

1. To have an accurate and complete picture of the FI's ICT operating environment, FIs should establish information asset management practices and maintain an inventory of all assets, both physical and logical, that include the following:

1.1. identification of information assets that support the FI's business and service provision, including asset type, format, location, backup information (where applicable), license information and business value.

1.2. classifying information assets based on their critical importance.

1.3. determining the ownership of information assets, as well as the roles and responsibilities of the staff who manage these assets. The asset owner is responsible for:

1.3.1. ensuring that information and assets related to information processing are classified according to sensitivity

1.3.2. establishing and regularly reviewing access and classification restrictions; and

1.3.3. establishing policies, standards and procedures to manage information assets based on their criticality.

Article 7
Management of third-party service providers

1. Without prejudice to the outsourcing regulation, before entering into contractual agreements or partnerships with third parties, the FI should assess its exposure to technological risks that may affect the confidentiality, integrity and availability of ICT systems and data, and manage such exposures throughout the life cycle of the third parties. In addition, it should have an appropriate exit strategy to address planned and unplanned departures from the technologies in use.
2. To ensure the continuity of ICT services and ICT systems, and without prejudice to other applicable requirements in accordance with the outsourcing regulation, the FI should ensure that contracts and service level agreements (both for normal circumstances and in the event of service disruption) with providers (outsourcing service providers, group entities or third party providers) include the following:

   2.1. appropriate and proportionate objectives and measures relating to information security, including requirements such as minimum cybersecurity requirements; specifications of the FI data lifecycle; any requirements relating to data encryption, network security and security monitoring processes, as well as the location of data centres, and

   2.2. operational and security incident handling procedures, including escalation and reporting.
3. The FI should monitor and seek assurance on the level of compliance of these providers with the FI's security objectives, measures and performance targets.
4. On an ongoing basis, the FI must maintain a register of all third-party service providers (including cloud services) and ensure that these providers maintain a high standard of care in protecting data confidentiality and integrity, as well as in ensuring system availability.

Article 8
Review of competencies and background

1. The FI should ensure that personnel, including contractors and service providers, have the required level of competence and skills to perform ICT functions in an ICT environment, to

manage technological risks. All ICT staff should have detailed job descriptions of duties and responsibilities to ensure that roles, responsibilities and required skills are adequately defined.

2. Background checks should be conducted on personnel with access to FI data and ICT systems to mitigate insider risk, including the risk of data breaches, sabotage and fraud by staff, contractors and service providers.

3. The FI must document the processes in accordance with this article to meet the requirements under this article.

Article 9
Information security awareness and training

1. FIs should establish a comprehensive ICT security awareness training program to maintain a high level of awareness among all FI staff. The training program should, at a minimum, include information on the prevailing cyber threat environment and its implications, the FI's ICT security policies and standards, and each individual's responsibility for safeguarding information assets. All personnel should be aware of applicable laws, regulations, and guidelines relating to the use of and access to information assets.

2. The training program must be conducted at least once a year for all staff, contractors, and service providers who have access to the FI's critical information assets.

3. The BD should undergo training to increase awareness of the risks associated with the use of technology and to reinforce their understanding of TRM practices.

4. The training program should be reviewed periodically to ensure that its content remains current and relevant. The review should take into account changes in the FI's ICT security policies, prevailing and emerging risks, the evolving cyber threat environment, lessons learned from previous training initiatives, and any training needs identified through behavioral observations, e.g. unannounced phishing tests on staff.

Article 10
Budget forecast

1. FIs should allocate sufficient budgetary funds to meet the appropriate level of cyber preparedness.

2. The cybersecurity budget should be independent of the FI's overall ICT budget, to ensure that business-related systems developments do not compete for resources allocated to protecting ICT systems.

3. When allocating the budget for each year, the training needs of information systems/cybersecurity staff should also be taken into consideration.

CHAPTER III
TECHNOLOGY AND CYBER RISK MANAGEMENT

Article 11
Risk management framework

1. The FI should establish a Risk Management Framework to effectively address ICT and cyber risks. Appropriate governance structures and processes should be established, with well-defined roles, responsibilities and reporting lines across all different organizational functions.
2. All identified technological risks should be assigned to risk owners, responsible for establishing and implementing appropriate risk management measures.
3. The risk management process should be executed repeatedly and regularly, including the following components:
   3.1. risk assessment, consisting of risk identification and analysis, to understand the risks faced by the FI;
   3.2. addressing risk, focusing on implementing risk mitigation measures that protect the confidentiality, integrity and availability of information assets; and
   3.3. risk monitoring, review and reporting, enabling stakeholders to immediately identify and communicate changes in risks.
4. Given that business, IT environments and the cyber threat environment evolve over time, the FI should regularly review the adequacy and effectiveness of its risk management framework and implement corrective measures as necessary.
5. The FI must document the risk management methodology in use and have it approved by the Board of Directors.
6. The FI should comprehensively document all iterations of the risk management process and their results, such as assessment criteria, data used, risk registers and remediation plans.
7. As a minimum, a summary report on the results of the risk management process, a risk register, and a detailed remediation plan should be prepared for board approval each year.
8. Technological Risk Management (TRM) should include all integrated information systems of the FI at all stages of their development.
9. Information system risk management should include an annual awareness plan for FI employees on the appropriate use of services provided through the FI's information system.

Article 12
Risk assessment

1. At least once a year or in the event of any significant changes to the ICT security requirements, the FI shall conduct a risk analysis of the ICT systems to ensure that this risk is kept within the tolerance limits in relation to the FI's activity. The results of the risk analysis shall be documented.
2. During the risk identification process, the FI should:

2.1. identify threats to its information assets;

2.2. identify vulnerabilities that can be exploited by threats;

2.3. identify existing controls; and

2.4. identify the potential consequences in different scenarios if threats exploit the identified vulnerabilities. When identifying potential consequences, the FI should consider financial, operational, legal, reputational and regulatory factors

3. During the risk analysis process, the FI should assess

3.1. the likelihood of threats exploiting identified vulnerabilities;

3.2. the magnitude of the consequences if threats exploit the identified vulnerabilities, and

3.3. assign a risk level metric to each risk, based on these assessments.

Article 13
Risk management

1. The FI should develop and implement risk mitigation measures that are consistent with the criticality of the information assets and the accepted level of risk tolerance.
2. The FI should assess whether the risks have been reduced to an acceptable level after the implementation of the mitigating measures. The criteria and approval authorities for accepting the residual risk should be clearly defined and should be consistent with the FI's risk tolerance.
3. Where possible, the FI should consider insurance coverage for various insurable technologies to mitigate financial impacts, such as recovery and compensation costs.

Article 14
Risk monitoring, review and reporting

1. The FI should establish a process for assessing and monitoring changes in risk.
2. Significant risks should be closely monitored and reported to the Board and senior management. The frequency of monitoring and reporting should be commensurated with the level of risk.
3. To facilitate risk reporting to management, technology risk metrics should be developed to highlight information assets with the highest risk exposure. These metrics should take into account risk events, audit findings, and relevant regulatory requirements.

Article 15
Project management framework

1. For large projects, a project steering committee should be established to ensure their effective oversight and governance.
2. A project management framework should be established to ensure consistency in project management practices and the delivery of results that meet project objectives and requirements. The framework should cover policies, standards, procedures, processes, and activities from project initiation to closure.

3. Detailed documentation of ICT projects should be created, maintained and approved by the relevant business and ICT management. The documentation should define the business case, scope and budget of the project, as well as the main phases, activities and deliverables for each phase of the project. The roles and responsibilities of the staff involved in the project should be clearly defined.

Article 16
Acquisition of IT systems

The FI should establish standards and procedures for evaluating and selecting suppliers to ensure that the selected supplier is qualified and capable of meeting the project requirements. The level of evaluation should be consistent with the importance of the project expectations for the FI.

Article 17
System development life cycle and security by design

1. The FI should establish a framework to manage the systems development life cycle (SDLC) to clearly define the processes, procedures, and controls at each stage of the life cycle, such as inception/planning, requirements analysis, design, implementation, testing, and acceptance. Standards and procedures for the different stages should be maintained.
2. The FI should incorporate security specifications into the design of systems, conduct ongoing security assessments, and adhere to security practices throughout the systems development lifecycle. Security requirements should cover key control areas, such as access control, authentication, authorization, data integrity and confidentiality, activity logging, security event tracking, and exception handling. The systems development lifecycle should include the IT security function at every stage of the lifecycle.

Article 18
System requirements analysis

1. The FI should identify, define and document the functional requirements for IT systems. In addition to functional requirements, key requirements such as system performance and security controls should be defined and documented.
2. When determining security requirements, the FI should assess the potential threats and risks associated with its IT systems by determining the level of security necessary to meet its business needs.

Article 19
Systems design and implementation

1. As part of the design phase, the FI should review the proposed architecture and design of the IT system including the IT and information security controls to be built into the system, to ensure compliance with the specified requirements.

2. The FI must verify that the requirements from the systems design are met during the design and implementation of the systems. Any changes or deviations from the defined requirements must be approved by the relevant stakeholders.
3. Relevant experts in the field should be engaged to participate in the review of the project.

Article 20
System testing and acceptance

1. A methodology for testing the system should be defined. The scope of testing should cover business logic, system functionality, security controls, and system performance under various load and stress conditions. A test plan should be defined and approved prior to testing.
2. Issues identified during testing, including system defects or software errors, should be documented and addressed appropriately. Major issues that could have a negative impact on FI operations or customer service delivery should be reported to the project steering committee and addressed prior to deployment into the production environment.
3. All test results must be documented and approved by the relevant stakeholders.
4. As part of project planning, quality metrics of expected performance should be determined.
5. An independent entity should provide quality assurance for large projects and there should be no conflict of interest between the entity and the developer.

Article 21
Secure coding, source code review, and application security testing

1. The FI should adopt standards on secure coding, source code review, and application security testing.
2. These standards should cover secure programming practices, input data validation, output data encoding, access controls, authentication, cryptographic practices, and error and exception handling.
3. Policies and procedures should be established on the use of third-party and open source software code to ensure review and testing before integration into the FI software.
4. To facilitate timely correction of vulnerabilities, the FI should maintain a log of updates and reported vulnerabilities of third-party and open source software code that is included in its software.
5. The FI must ensure that its software developers are trained or have the necessary knowledge and skills to implement secure coding and application security standards during application development.
6. The FI should create a comprehensive strategy to conduct application security validation and testing.
7. All software problems and bugs discovered by source code review and application security testing should be recorded and traceable. Major software problems and bugs should be corrected before deployment.

Article 22
DevSecOps Management

1. If a DevSecOps approach is adopted, the FI should ensure that the relevant activities and processes are consistent with the system development lifecycle framework and IT service management processes (e.g., configuration management, change management, or software release management).
2. The FI should implement appropriate security measures and implement segregation of duties for software development, testing, and release functions in its DevSecOps processes.

Article 23
Application Programming Interfaces (APIs)

1. The FI must establish sufficient safeguards to manage the development and provision of Application Programming Interfaces (API) for the secure provision of services. All requirements for secure coding, source code review, and application security testing are equally applicable to API development.
2. Before allowing third parties to connect to its IT systems via API, the FI must conduct a risk assessment and ensure that the security controls for each API are consistent with the sensitivity and business criticality of the data being exchanged, as well as the confidentiality and integrity requirements of this data.
3. IFs should establish security standards for the design and development of secure APIs. The standards should include measures to protect API keys or access tokens, which are used to authorize access to the API to exchange confidential data. A reasonable time frame for the expiration of access tokens should be defined and enforced to reduce the risk of unauthorized access.
4. Strong encryption standards and key management controls should be adopted to secure the transmission of sensitive data through APIs.
5. Rigorous security testing of the API must be performed between the FI and the related parties before it is deployed.
6. Sessions involving related parties must be recorded by the IF. The logs must include details such as the identity of the party making the API connection, the date and time, as well as the transactions executed and data accessed. These logs must be available for audit purposes as needed.

CHAPTER IV
IT SERVICES MANAGEMENT

Article 24
Documentation

1. The FI must maintain complete and up-to-date documentation of infrastructure, applications and systems, security, operational factors and other important factors related to IT activity.
2. Systems and services should be documented in a way that enables replacement staff to run IT operations with minimal disruption, which can be achieved through the development of comprehensive operations manuals.
3. All updates should be recorded and documentation should be promptly revised to reflect any changes in infrastructure, applications, or regulatory requirements.
4. The FI should implement role-based access controls to restrict access to sensitive documentation and ensure that only authorized personnel can view or modify documents.
5. All critical documentation should be reviewed at least once a year or whenever there are significant changes and approved by senior management.

Article 25
Physical checks

1. The FI should take the necessary protective measures to prevent any unauthorized physical access, interference or damage to the information, information processing equipment and operations of the FI, based on international standards and best practices. Regular audits should be carried out to ensure the integrity and security of physical assets.
2. The FI must establish access and work procedures for secure areas for all employees and external parties. Secure areas must be protected through access controls to ensure that only authorized employees have access.
3. The FI must maintain comprehensive documentation of physical security policies, procedures and controls and keep detailed records of all security assessments, incidents and maintenance activities.
4. The FI must implement multi-factor authentication (MFA) for access to secure areas and maintain detailed logs of all access to secure areas and review them regularly.
5. All access by third parties and visitors must be recorded and they must be accompanied at all times while within secure areas.
6. All secure areas should be equipped with surveillance cameras and they should provide full coverage of the area, ensuring that no spaces are left uncovered.
7. The surveillance system must comply with relevant privacy regulations and standards, including data protection protocols, to protect recorded footage.
8. The FI must implement all necessary controls in the data center to effectively manage environmental factors, including but not limited to temperature extremes, fire detection and suppression systems.
9. The FI must provide systems that ensure continuity of power supply, such as UPS (Uninterruptible Power Supply), backup generators or similar, to ensure that there is no interruption of operations during power outages.

Article 26
Software as a Service

1. Software as a Service (SaaS) should be managed through appropriate measures. The FI should implement encryption for data at rest and in transit to protect sensitive information and strong key management practices to secure encryption keys. The FI should implement formal configuration and documentation processes.
2. The FI should use identity and access management solutions or processes to implement strict access controls, endpoint protection, and security monitoring to protect against data breaches and malware/virus infections.
3. The FI should conduct regular risk assessments specific to software management and SaaS applications, to identify vulnerabilities and threats.
4. The FI must maintain comprehensive documentation of all software management processes, including development, testing, deployment, and security measures.

Article 27
Configuration management

1. The FI must develop an effective configuration management process to ensure effective and compliant management of IT assets and services, including but not limited to hardware, software and documentation;
2. The FI must establish criteria for identifying and classifying Configuration Items (CIs), and maintain a form of CI registry;
3. The configuration management process should be integrated with change management processes to ensure that all changes to the CA are recorded, evaluated and managed appropriately;
4. The FI must implement mechanisms to track and report the status of configuration data.
5. Configuration management practices will be subject to regular reviews and assessments to identify opportunities for improvement;
6. The FI should use standardized software configurations and images whenever possible.

Article 28
Technology refresh management

1. The FI should draft and maintain a Technology Update Strategy that describes the approach to planning and executing technology refreshes.
2. The FI should establish procedures for assessing the necessity of technological upgrades. This includes assessing the performance and reliability of existing technology.
3. All software (including operating systems) and hardware (including network equipment) must be within the lifecycle period covered by the provider's active support (including extended support), if applicable.

4. Maintenance or licensing contracts must be in place for access to updates, minor improvements, and other critical maintenance features.
5. Risk assessments for hardware and software approaching End-Of-Support (EOS) dates should be conducted to assess the risks of their continued use, and effective risk mitigation measures should be implemented.
6. The Technology Refresh Management process should undergo regular reviews and assessments to identify areas for improvement and optimize refresh practices.

Article 29
Patch Management

1. The FI should develop and implement a comprehensive Patch Management Policy. This policy should define the principles and procedures that govern the identification, assessment, deployment, and verification of patches.
2. FIs should establish procedures for identifying relevant patches. This includes purchasing patches from vendors and manufacturers that address security vulnerabilities or provide updates.
3. A formal assessment process should be implemented to assess the impact, risk, and benefits of patches, as well as the recovery plan, prior to deployment. This assessment should include testing patches in a controlled environment to ensure compliance.
4. All changes related to patch deployment should be documented, including patch details, deployment actions, and any issues encountered.
5. The FI must implement procedures to verify that patches have been applied correctly and effectively address identified vulnerabilities or problems.
6. Patch Management activities should be integrated with Change Management processes to ensure that patch deployments are planned, approved, and documented in accordance with change management protocols.

Article 30
Change management

1. The FI must establish appropriate Change Management Policies and Procedures to control changes in the IT environment in order to minimize disruptions.
2. IFs should establish a formalized change management mechanism, overseen by a Change Advisory Board (CAB), comprised of key stakeholders, including business management and IT, to approve, review, and prioritize changes. All changes should be properly tested and approved, and the results of the testing should be accepted and approved before the changes are deployed to the production environment.
3. All intended changes should be well documented and risk assessed, and change requests should be properly recorded, categorized, and prioritized. The risk analysis should cover factors such as security and the implications of the changes in relation to other information assets.

4. Before implementing changes, a backup of information assets should be made and a recovery plan should be created to revert to the previous state if any problems arise during or after implementing the change. This plan should be tested as part of the project and implementation life cycle.
5. The FI should clearly define procedures for assessing, approving and implementing emergency changes. Approvers of emergency changes should be identified and emergency changes should be monitored and recorded.
6. The FI should conduct a post-implementation review to ensure that the changes achieve the desired results.

Article 31
Incident management

1. The FI must implement a comprehensive Incident Management Policy and relevant processes and procedures for handling, categorizing and prioritizing IT incidents, including cybersecurity incidents.
2. The FI must develop and regularly update an incident response plan, establish an incident response team and equip them with the necessary tools and resources to handle and manage incidents;
3. The FI defines the roles and responsibilities of staff and external parties involved in recording, analyzing, escalating, deciding, resolving, and monitoring incidents.
4. The FI should maintain an incident log in order to track and manage incidents throughout their lifecycle, from detection and recording to resolution and closure. Incidents should be categorized based on their type, criticality, and impact.
5. To improve response strategies and ensure compliance with agreed service levels, regular reviews and assessments of incident data should be conducted to identify trends in response strategies.
6. The FI must implement incident reporting mechanisms by users;
7. The FI must ensure the availability of tools or mechanisms for incident detection, analysis and response.
8. The FI must ensure the restoration of affected systems and services to normal operation and ensure that they are secure before returning them to service;
9. The FI must ensure effective communication within the institution during and after an incident, including communication with external parties. The FI must ensure that a communication plan is developed and reviewed regularly.
10. The FI must notify and report the incident to the CBK, no later than 4 hours after its discovery. The initial report or notification must provide information on the significant threat, as well as the affected systems. An interim report must be submitted within 72 hours and the final report within 30 days. Templates for submitting the report are provided in the Annexes to this document.

Article 32
Post-incident review and lessons learned

1. The FI must maintain detailed records of the incident handling process, including actions taken and decisions made.
2. The FI prepares and submits reports to relevant stakeholders, including governing and regulatory bodies.
3. The FI should review incident response policies and procedures based on feedback and lessons learned from incidents.

Article 33
Identity and access management

1. The FI should establish an appropriate policy for identification and access management. The policy should specify the password policy, multi-factor authentication and criteria for privileged access, including third parties. The FI should implement strong password controls for user access to IT systems and two-factor or multi-factor authentication for system administration accounts and remote access.
2. The FI should implement principles such as "never alone", "segregation of duties" and "least privilege" when granting staff access to information assets.
3. System access rights and privileges should be granted according to the roles and responsibilities of staff and third parties.
4. The FI must implement a user access management process to grant, modify, and revoke access rights to information assets. Access rights must be authorized and approved by appropriate parties, such as the owners of the information assets.
5. The FI should ensure that users are granted access rights only on a need-to-use basis. Access rights that are no longer needed, such as due to a change in a user's job responsibilities or employment status, should be revoked or deactivated immediately. Service providers with access to the FI's information assets should be subject to the same monitoring and access restrictions as the FI's personnel.
6. Access to privileged accounts, such as developer access to a work environment to resolve a problem, should be granted only on a need-to-use basis and for the minimum period necessary; the activities of these accounts should be recorded and reviewed as part of the ongoing monitoring of the FI.
7. The FI should conduct periodic reviews of user access rights at least every 6 months, to ensure that they remain appropriate in order to identify and correct any unauthorized access.
8. The FI must maintain comprehensive logs of access events to support monitoring, auditing and compliance.

Article 34
Network management

1. The FI should create and document comprehensive network security policies.
2. The FI must install network security devices, such as firewalls, to secure the network between the FI and the internet, as well as connections to third parties.
3. The FI should implement strict access controls on network equipment and infrastructure, ensuring that only authorized personnel can make changes or access sensitive data. Network access control rules on network equipment should be documented and reviewed regularly.
4. IF information assets should be grouped into network segments based on the criticality of the systems, the functional role of the system, or the sensitivity of the data.
5. Implement network access controls to detect and prevent unauthorized devices from connecting to its network and ensure that sensitive data transmitted over the network is encrypted to protect it from eavesdropping and unauthorized access.
6. The FI should consider isolating internet browsing activities from its end devices through the use of physical or logical controls to minimize exposure to cyber-attacks.
7. The FI must implement an effective Distributed Denial of Service (DDoS) protection solution to detect and respond to various types of such attacks.
8. The FI should conduct regular risk assessments of the network architecture, including network security design, as well as system and network interconnections periodically to identify potential cybersecurity vulnerabilities.
9. The FI must create and maintain recovery plans for network configurations, devices, and data to ensure business continuity and compliance.
10. The FI should take protective measures and establish mechanisms to protect the internal network from threats coming from external sources, such as cyber-attacks and other attempts to breach the internal infrastructure. These protective measures should include:

    10.1. detailed documentation of network end devices; and

    10.2. policies and procedures for access and traffic monitoring.

Article 35
Virtualization security management

1. The FI should document and implement security policies specifically tailored to virtualization technologies. Such policies should cover the security, creation, distribution, storage, backup, use, retrieval, and destruction of virtual images.
2. The FI should ensure that security standards are established for all components of a virtualization solution. Ensure that only authorized personnel have access to virtualization layers (hypervisors) and host operating systems, in accordance with the principle of least necessary rights.
3. The FI should use network segmentation and isolation techniques to separate virtual environments.
4. The FI must maintain an accurate and up-to-date inventory of virtual resources and configurations.

5. IF ensures that data stored within virtual machines is encrypted and that appropriate data backup and recovery procedures are developed to protect against data loss and breaches.
6. FIs should conduct regular audits of virtualization security practices to ensure compliance with internal policies and regulatory requirements.

Article 36
Data security and privacy

1. The FI should develop comprehensive data loss prevention policies and adopt measures to detect and prevent unauthorized access, modification, copying or transmission of its sensitive data. Data in transit, data at rest and data in use should be considered.
2. The FI must implement appropriate measures to prevent and detect data theft, as well as unauthorized modifications to systems and end devices. Monitoring mechanisms must be implemented to detect potential incidents of data loss or policy violations.
3. The FI should establish a data classification policy to categorize data based on sensitivity and compliance requirements and implement strict access controls to ensure that only authorized personnel can access sensitive data.
4. The FI must ensure that sensitive data is encrypted both in transit and at rest, and is protected by strong access controls.
5. The FI should develop a strategy for restoring key data in cases where data in use and online backups are compromised.
6. The FI must ensure that systems managed by service providers comply with their FI data security policies and regulatory obligations.
7. To prevent data leakage, appropriate controls should be implemented in non-active work environments.
8. The FI should limit the use of sensitive data from active work environments to non-active work environments. At least data anonymization or masking should be implemented, when active work environment data must be used in test environments.
9. The FI must define and implement data retention policies that comply with regulatory requirements, and data must be permanently deleted from storage media, systems and end devices, before destruction or redistribution.

Article 37
Managing the security of personal devices in the work environment

1. The FI should create a clear and comprehensive policy for personal devices in the work environment (BYOD – Bring Your Own Device) that outlines acceptable use, security requirements, and user responsibilities.
2. The FI must conduct a comprehensive risk assessment and appropriate security measures must be taken when using personal devices in the work environment (BYOD).

3. The FI must implement controls and measures to prevent data loss on personal computers or mobile devices used to access the FI's information assets.
4. The FI must use encryption for sensitive data stored on personal devices and for data transmitted between these devices and the institution's resources.
5. The FI must provide the ability to remotely wipe data from personal devices in the event of loss, theft, or employee termination.
6. The FI must implement security measures for devices accessing its network, such as firewalls, VPNs, and intrusion detection systems to monitor and protect against threats.
7. The FI ensures that institutional data is kept separate from personal data on the device, through the use of containerization or mobile device management solutions.

Article 38
Safe disposal management

1. The FI must ensure that appropriate procedures are in place for the disposal of IT assets, both from a data privacy and environmental perspective.
2. The FI should conduct regular risk assessments to identify potential threats associated with data destruction and create mitigation strategies.
3. The FI should define acceptable disposal methods for different types of data (e.g., physical destruction, data erasure) in physical and virtual environments to ensure that the data cannot be reconstructed and should maintain complete documentation of the destruction processes and results.
4. The FI should regularly review and update its safe disposal management practices, based on new threats, regulatory changes and best practices.

CHAPTER V
CYBER SECURITY OPERATIONS

Article 39
Cyber threat intelligence and information sharing

1. The FI should establish a process to collect, process and analyse information related to cybersecurity for its relevance and potential impact on its business and IT environment. Information related to cybersecurity should include cyber events, cyber threat intelligence and information on system vulnerabilities. This should include voluntary and collaborative industry networks or national information sharing networks, where such networks exist.
2. The FI should consider implementing cyber intelligence monitoring services and actively participate in cyber threat information sharing agreements with trusted parties.

Article 40
Cyber events monitoring and detection

1. To facilitate the continuous monitoring and analysis of cyber events, as well as the detection and rapid response to cyber incidents, the FI should perform monitoring, detection, response and recovery functions. In this regard, the FI should consider establishing a Security Operations Center (SOC) or acquiring managed security services in accordance with Article 3 of this Regulation. Processes, roles and responsibilities for security operations should be defined.
2. The FI should consider granting pre-delegated authority for certain emergency actions to contain incidents and limit spread. This may include, but is not limited to, emergency equipment or service interruption when there is no time to assemble the incident response team/plan.
3. A process for collecting, processing, reviewing, and storing system logs should be established to facilitate the security monitoring operations of the FI. A baseline of minimum logging requirements should be established (e.g., recording successful and unsuccessful login events, privilege changes, etc.). These logs should be protected from unauthorized access.
4. To facilitate the identification of anomalies, the FI should create a baseline profile of the routine activities of each IT system and analyze the system activities against the baseline profiles. The profiles should be reviewed and updated regularly.
5. To identify suspicious patterns or anomalies of system activity in system logs, correlation of multiple recorded events should be performed.
6. A process should be established to immediately escalate suspicious or anomalous system activities or user behavior to appropriate stakeholders.

Article 41
Cyber incident response, management and reporting

1. The FI should establish a cyber-incident response and management plan to rapidly isolate and neutralize a cyber-threat and safely resume affected services. The plan should outline communication, coordination, and response procedures to address potential cyber threat scenarios and should be integrated with broader crisis response and management plans across the FI.
2. As part of the plan, the FI must establish a process to investigate and identify the security or control deficiencies that led to the breach. The investigation must also assess the full extent of the impact on the FI and any related third parties.
3. Information from cyber intelligence and lessons learned from cyber incidents should be used to improve existing controls or improve the cyber incident management plan.

Article 42
Incident reporting

Cyber incidents and technological failures must be reported to the relevant Regulatory Authorities, according to 0 - Incident management of this regulation.

CHAPTER VI
RESPONSE AND RECOVERY

Article 43
System availability

ICT systems should be designed and implemented to achieve a level of system availability that is consistent with its business needs. Acceptable levels of service or system availability should be defined for each business function and recorded in internal or external service level agreements.

Article 44
Business continuity management and disaster recovery

1. FIs should establish a sound business continuity management process to maximize their ability to provide services continuously, achieve their availability objectives set out in their service level agreements, and minimize losses in the event of severe business disruptions.
2. As part of sound business continuity management, FIs should conduct a Business Impact Analysis (BIA) by analyzing their exposure to and impact from business disruptions. A range of scenarios should be considered, including the most severe but plausible ones.
3. The business impact analysis should also consider the importance of identified and classified business functions, supporting processes, third parties and information assets, as well as their interdependencies.
4. The FI should determine system recovery time objectives and recovery point objectives that are consistent with the results of the business impact analysis.
5. FIs should ensure that the availability characteristics of ICT systems are consistent with their business impact analysis results. For example, redundancy may be implemented for some critical components to prevent disruptions caused by events affecting these components.
6. Based on the FI’s business impact analysis, FIs should develop plans to ensure business continuity and disaster recovery. These plans, which should be documented and approved by their management bodies, should specifically consider the risks that could impact ICT systems and services. FIs should coordinate with relevant internal and external stakeholders, as appropriate, when developing these plans.
7. Staff should be trained to use the plans, and the plans should be reviewed, updated and tested at least annually or after significant changes to ICT systems or business processes.

Article 45
Disaster recovery plan test

1. Relevant stakeholders, including those in the business and ICT functions, should participate in business continuity and disaster recovery tests to familiarize themselves with recovery processes and determine whether systems are functioning as expected.

2. A business continuity/disaster recovery test should be based on a test plan that includes objectives and scope, test scenarios, with details of activities to be performed during and after testing, and criteria for measuring test success.
3. Testing should include various potential outage scenarios, including complete and partial primary data center outages and major system failures. It should also address recovery dependencies between different information assets, including those managed by third parties.
4. Where information assets are managed by service providers, the FI should assess their disaster recovery capabilities and ensure that disaster recovery arrangements for these information assets have been established, tested and verified to meet the FI's business needs. The FI should engage its service provider to test recovery steps that require coordinated actions.

Article 46
Backup and recovery

1. The FI should establish policies and procedures for regular backups that enable recovery in the event of system outage, data corruption or deletion. Archiving the data for long-term storage should be included in the policies and procedures.
2. To ensure that data availability is consistent with the FI's business requirements, the FI should establish a policy to manage the backup data lifecycle. This should include the frequency of data backup, the data retention period, the number of online and offline backups, the management of data storage mechanisms, and the secure destruction of backup media at the end of their lifecycle.
3. To address ransomware risks, FI should consider creating air-gapped or immutable backups.
4. The FI should periodically test its system recovery and data backups to verify the effectiveness of the recovery procedures. For critical systems, recovery tests should be performed at least every six months, while for non-critical systems, tests should be performed at least once a year.
5. To protect backups from unauthorized access and modification, the FI must ensure that any confidential data stored on backup media is secure (e.g., encrypted).
6. Backups of customer data and other data critical to the operation of the FI should be redundant (e.g., at least two equivalent copies) and stored in separate, secure locations that are unlikely to be affected by the same disaster.

Article 47
Data center

1. The FI should conduct a Threat and Vulnerability Risk Assessment (TVRA) for its data centres (DCs) to identify potential vulnerabilities, weaknesses and safeguards that should be put in place to protect the data centres (DCs) from physical and environmental threats. In addition, the assessment should take into account the political and economic climate of the country in which the DCs are located. The Threat and Vulnerability Risk Assessment should be reviewed whenever there is a significant change in the threat environment or when there is a material change in the data centre environment.

2. The FI should provide sufficient redundancy for power, network connectivity, cooling and other electrical and mechanical systems within the DC to eliminate the risk of single points of failure. Attention should be paid to the following:

   2.1. diversification of data communications, network paths and suppliers;

   2.2. deployment of power equipment, such as UPS and backup generators, and

   2.3. implementing appropriately redundant cooling equipment (e.g., cooling towers, chilled water supply, and computer room air conditioning units) to control temperature and humidity levels in the data center and prevent potentially harmful fluctuations to the systems.

3. As part of the data center's environmental controls, the FI should implement fire detection and suppression devices or systems, such as smoke or heat detectors, inert gas extinguishing systems, and wet or dry water sprinkler systems.

4. The secondary data center or disaster recovery center of the FI should be geographically separated from its primary or operational center. This will ensure that disruptions to basic infrastructure (e.g., telecommunications and power) and/or environmental hazards at a given location do not impact both locations simultaneously.

5. The physical and environmental security controls of the DC must be monitored 24/7.

6. Response plans and procedures for physical and environmental incidents at the DC should be defined and tested for a certain level of escalation.

7. The DC should have appropriate physical access controls. Best practices include:

   7.1. granting access to staff on a need-to-know basis, immediately revoking access when it is no longer needed;

   7.2. implementing appropriate notification and approval protocols for visitors to the data center. All visitors must be accompanied by authorized staff at all times while in the data center;

   7.3. securing and monitoring physical access points to the data center at all times;

   7.4. limiting and monitoring access to equipment racks;

   7.5. ensuring that staff with physical access to equipment racks do not also have access to information systems;

   7.6. limiting access to keys and other physical devices only to authorized staff, promptly replacing or changing them if they are misplaced, lost or stolen, and

   7.7. separating common areas from sensitive security areas.

CHAPTER VII
SCANNING, TESTING, EXERCISES AND INTERRUPTION

Article 48
Vulnerability scanning

The FI should establish a process for regular vulnerability scanning to identify security vulnerabilities and promptly address the risks associated with them. The frequency of scanning should be consistent with the criticality of the IT systems and the security risk to which they are exposed.

Article 49
Penetration test

1. The FI should conduct penetration test to gain a deep understanding of its cybersecurity protection.
2. The external digital services of the FI must be subject to penetration tests at regular intervals. For FIs categorised according to Article 3 paragraph 1, penetration tests must be carried out at least once a year and after any major changes to the underlying systems. For all other FIs, penetration testing must be carried out at least every two years and after any major system modification.
3. Testing must be carried out by persons with sufficient knowledge and expertise, as well as competent to carry out such activities.

Article 50
Incident response exercises

1. The FI should conduct regular cyber exercises to validate cyber incident response and recovery procedures, including communication plans. These exercises may include a tabletop exercise and attack simulations. In addition, they may be combined with penetration testing and BCP/DRP (business continuity planning/disaster recovery planning) testing.
    1.1. For the purposes of this article, a major cyberattack could be an outage scenario in a disaster recovery planning test.
2. Depending on the objectives of the exercise, the FI should involve relevant stakeholders, including senior management, business units, corporate communications specialists, crisis management teams, service providers, and technical staff responsible for detecting, responding to, and recovering from cyber threats.

Article 51
Corrective measures management

1. FIs should establish a comprehensive corrective measures process to track and resolve issues identified through vulnerability scanning, penetration test, and cyber exercises. The process should include, at a minimum, the following:
    1.1. assessing the criticality and classifying a problem (including flagging and verifying false positives);
    1.2. time frame to solve problems of varying importance, and
    1.3. risk assessment and mitigation strategies to manage deviations from the framework.

CHAPTER VIII
INDEPENDENT WARRANTY

Article 52
Audit

1. The requirements set out in the Regulation on Internal Controls and Internal Audit of FIs apply to the audit of the information system.
2. The internal audit function should conduct internal audits of IT, cybersecurity controls, governance, compliance and outsourcing processes by auditors with sufficient knowledge, skills and competence in IT and security risks, to provide independent assurance of their effectiveness to the board and senior management. Auditors should be independent from within or outside the FI and the frequency and focus of such audits should be consistent with the relevant IT and security risks.
3. The FI's Board of Directors should approve the annual audit plan, including any IT audits and any material modifications thereto. The audit plan and its execution, including the audit frequency, should reflect and be proportionate to the inherent IT and security risks of the FI and should be updated. The scope and frequency of audits should be consistent with the criticality and risk profile of the information assets, functions and processes.
4. A formal follow-up process should be established, including provisions for timely verification and correction of critical IT audit findings.
5. High-risk observations and corrective actions taken should be reported to the Board of Directors without undue delay.
6. At a minimum, the FI should employ internal audit staff with the competence and skills to develop an annual technology risk audit plan and to understand the findings, risks, and recommendations of specialized external providers.
7. The IT field activity should be subject to at least an annual periodic review that focuses on risk-based methodology.
8. The FI should ensure that its technology risk auditors have the required level of competence and skills to effectively assess the adequacy of implemented IT policies, procedures, processes and controls.

CHAPTER IX
MANAGEMENT OF OUTSOURCED TECHNOLOGY SERVICE PROVIDERS

Article 53
Proportionality

When implementing the requirements set out in this regulation, FIs should consider the complexity of the outsourced functions, the risks arising from the outsourcing arrangement, the

criticality of the outsourced function and the potential impact of outsourcing on the continuity of their activities.

Article 54
Governance

1. The delegation of functions or the use of technology service providers (TSP) does not relieve the board of its responsibilities. FIs remain responsible and fully accountable for fulfilling all their regulatory obligations, including the ability to oversee the outsourcing of critical or important functions.
2. The FI must ensure that technology service providers (TSPs), including for outsourcing, do not result in increased technological and cyber risk.
3. For proper governance of the delegation of functions or the use of technology service providers, the FI must:
   3.1. clearly assign responsibilities for the documentation, management and control of outsourcing agreements;
   3.2. allocate sufficient resources to ensure compliance with all legal and regulatory requirements, including guidelines and documentation and monitoring of all external agreements;
   3.3. establish an outsourcing function or designate a senior member of staff who reports to the board (e.g., a key function holder) and who is responsible for managing and overseeing the risks of outsourcing arrangements as part of the institution's internal control framework and overseeing the documentation of outsourcing arrangements.
4. When outsourcing, the FI must ensure at least the following:
   4.1. approving and implementing decisions related to its business activities and critical or important functions;
   4.2. maintaining the orderly development of its business and providing financial services;
   4.3. identification, assessment, management and adequate mitigation of risks arising from outsourcing;
   4.4. where applicable, appropriate confidentiality arrangements regarding data and other information;
   4.5. maintaining an appropriate flow of relevant information with service providers;
5. In the event of an unplanned interruption of contracted services, critical or important functions, the institution shall take at least one of the following actions, within an appropriate timeframe:
   5.1. transfer of the function to alternative service providers;
   5.2. reintegration of the function into the institution; or
   5.3. the cessation of business activities that depend on the function; and
   5.4. When personal data are processed by service providers located in third countries, the data is processed in accordance with the Law on Personal Data Protection.

Article 55
Risk assessment

1. The FI must determine whether the delegation by an institution of the performance of processes, services or activities to a service provider falls under the definition of outsourcing.
2. For the purposes of this Regulation, the following determinations shall not be considered as outsourcing:
   2.1. global financial communication services (e.g., SWIFT) if the main information system resources necessary for the provision of such a service are within the institution;
   2.2. the function that is legally required to be performed by a service provider (e.g., statutory audit);
   2.3. market information services (e.g., providing data from Bloomberg, Moody's, Standard & Poor's, Fitch);
   2.4. global network infrastructures (e.g., Visa, MasterCard) and telecommunications services;
   2.5. clearing and settlement agreements between clearing houses, central counterparties and settlement institutions and their members;
   2.6. global financial messaging infrastructures subject to oversight by relevant authorities;
   2.7. correspondent banking services;
   2.8. the purchase of services that would not otherwise be performed by the institution (e.g. advice from an architect, provision of legal opinion and representation before the court and administrative bodies, cleaning, gardening and maintenance of the institution's premises, medical services, servicing of company cars, catering, vending machine services, administrative services, travel services, post office services, receptionists, secretaries and switchboard operators), goods (e.g. plastic cards, card readers, office supplies, personal computers, furniture) or services (e.g. electricity, gas, water, telephone lines);
   2.9. software which, being ready-made, is commercially available on the market and does not require significant adaptation; and
   2.10. other services similar to those specified in subparagraphs 2.1 to 2.9 of this paragraph, provided that the CBK gives a preliminary opinion that the provisions of this Regulation do not apply to the use of these services.
3. The FI should assess the potential operational risk of using a Technology Service Provider (TSP) and entering into a contractual arrangement. The FI should consider the results of the assessment to guide decisions on outsourcing services and take appropriate steps to avoid additional operational risks before entering into a contractual arrangement.
4. The FI should always consider a function as critical or important in the following situations:
   4.1. when a defect or failure in its performance would significantly harm the financial performance and continuity of the institution's activity.
   4.2. When operational tasks of internal control functions are outsourced, an assessment should be conducted to determine whether a failure to provide the contracted function or its

inadequate provision would adversely affect the effectiveness of the internal control function.

5. In order to manage outsourcing risk, it is necessary to determine the criticality or importance of the function to be outsourced.
6. The FI should define the criteria and define the methodology to assess the criticality or importance of a function, including its impact on regulatory compliance and licensing, impact on financial performance, contribution to operational sustainability and continuity of services, importance in maintaining customer trust and service quality, potential impact on the institution's reputation or position in the market and the degree of dependence on core business operations.
7. The assessment of importance or criticality is an ongoing process that should be performed at regular intervals. Regularly review the assessment of criticality or importance to ensure that it remains relevant as business conditions, regulations, and operations change over time.
8. The assessment of critical or important functions involves a structured approach to determine the importance of each function to the institution's operations and regulatory obligations. This assessment is essential for making informed decisions regarding outsourcing and ensuring that outsourcing arrangements do not compromise operational sustainability or regulatory compliance.

Article 56
Contractual relationship between the FI and a Service Provider

1. When entering into an agreement with a service provider, the FI should ensure that the scope and content of the contractual provisions are appropriate to the risks associated with outsourcing and to the scope and complexity of the outsourced functions.
2. Institutions must enter into a written agreement with a service provider, which must contain at least the following:
   2.1. a detailed description of the contracted function that is the subject of the agreement;
   2.2. the start date and end date of the fulfillment of contractual obligations;
   2.3. the financial obligations of the parties;
   2.4. provisions governing the manner in which an institution continuously monitors the performance of the function that is the subject of the agreement, including the types of reports that the institution must receive from the service provider and the frequency of their submission;
   2.5. the obligation of the service provider to notify the institution in a timely manner of all facts and changes in circumstances that have or may have a significant impact on the fulfillment of contractual obligations;
   2.6. the agreed service level and quality of the functions performed, including qualitative and, where applicable, quantitative performance objectives for the contracted function, which allow for timely corrective action to be taken by the institution;

2.7. where appropriate, the obligation of business secrecy and the obligation and manner of protecting confidential and personal data, including provisions regarding the access, availability, integrity, privacy and security of the relevant data;

2.8. where necessary, the location(s) where the contracted function will be provided and where the relevant data will be held, processed and stored, including a requirement to notify the institution if the service provider proposes to change the location(s);

2.9. provisions on whether subcontracting of the function is permitted;

2.10. the obligation of the service provider to provide services in such a manner that it is fully compliant with the relevant legislation of the Republic of Kosovo;

2.11. the obligation of the service provider to provide the CBK with access and on-site examination rights, in the manner specified in Article 5, paragraph 2, of this Regulation;

2.12. provisions ensuring that data owned by the institution can be accessed in the event of the dissolution or cessation of the service provider's business operations (e.g. bankruptcy, resolution of issues, liquidation or similar procedures);

2.13. provisions on whether the service provider must obtain a professional indemnity insurance policy and, if applicable, the level of insurance coverage required;

2.14. the obligation of the service provider to cooperate with the CBK as competent authorities and resolution authorities of the institution;

2.15. the duration of the contractual relationship or an indication that the agreement is of indefinite duration;

2.16. a description of the conditions for termination and/or cancellation of the agreement with notice periods set for the institution and the service provider;

2.17. the institution's rights to terminate or cancel an agreement with the service provider, if any, ordered by the CBK;

2.18. the choice of applicable law; and

2.19. method of resolving disputes.

3. When the FI and the service provider enter into an agreement for outsourcing critical or important functions, the agreement must, in addition to the content specified in paragraph 2 of this article, contain the following:

3.1. the obligation of the service provider to provide access and audit rights to the institution in the manner specified in Article 57, paragraph 2 of this Regulation;

3.2. provisions on the implementation and testing of business emergency plans;

3.3. the obligations of the service provider in the event of the transfer of the delegated function to another service provider or back to the institution, including obligations regarding data processing;

3.4. defining an appropriate transition period during which the service provider, after the termination or cancellation of the outsourcing agreement, will continue to provide the contracted function to mitigate the risk of disruptions; and

3.5. the obligation of the service provider to support the institution in the orderly transfer or reintegration of the function in the event of cancellation or termination of the contracting agreement

4. The contractual agreement should specify whether or not subcontracting of critical or important functions, or material parts thereof, is permitted.

5. If subcontracting of critical or important functions is permitted, institutions must determine whether the part of the function to be subcontracted is, as such, critical or important (i.e., a material part of the critical or important function) and, if so, record it in the register.

6. When an outsourcing agreement for critical or important functions includes the possibility of subcontracting, in addition to the content specified in paragraphs 2 and 3 of this article, that agreement must contain at least the following:

   6.1. the obligation of the service provider to notify the institution of any planned subcontracting, or material changes thereto, within a period that would allow the institution to carry out a risk assessment of the proposed changes and, where necessary, to object in due time to the planned subcontracting, or material changes thereto;

   6.2. The right to cancel/terminate the agreement when subcontracting increases risks for the institution or when the service provider subcontracts without notifying the institution and in other justified cases;

   6.3. when subcontracting involves the processing of personal data, the obligation of the service provider to obtain written authorization from the institution;

   6.4. the obligation of the service provider to supervise those services it has subcontracted;

   6.5. the conditions that must be met in the case of subcontracting;

   6.6. types of functions that cannot be subcontracted;

   6.7. the obligation of the service provider to seek written approval from the institution for any planned subcontracting, or material changes thereto, or the right to object to the planned contracting; and

   6.8. the obligation of the service provider to negotiate with the subcontractor on the rights of access and audit or examination on site in the manner specified in Article 57, paragraph 1 of this Regulation.

7. The FI may allow subcontracting only when the subcontractor undertakes to act in accordance with applicable law and regulatory requirements, to fulfill the relevant contractual obligations and to provide the institution and the CBK with the same access and audit or examination rights on site as those granted by the service provider in accordance with Article 57 of this Regulation.

8. The FI shall ensure that the service provider adequately supervises the sub-service providers, in accordance with the policy established by the institution. If the proposed sub-contracting could have material adverse effects on the sub-contracting arrangement of a critical or important function or would lead to a material increase in risk, including where the conditions in paragraph 7 of this Article would not be met, the institution shall exercise its right to object to the sub-contracting, if such a right has been agreed, and/or to terminate the contract.

Article 57
Rights of access and on-site audit or examination

1. The FI must ensure, within the outsourcing agreement with the service provider, that the service provider provides the CBK or any person appointed by the CBK for this purpose, the following:

   1.1. Timely and full access to business premises, including equipment, systems, networks, information and data used to provide the contracted function, including relevant financial information, personnel and external auditors of the service provider; and

   1.2. Conducting on-site examinations of a part of the service provider's activity that is or may be related to outsourcing, as well as on-site examinations of the performance of functions that are the subject of the agreement with the service provider, to enable it to monitor the contracted agreement and to ensure compliance with all applicable regulatory and contractual requirements.

2. Regarding the outsourcing of critical or important functions, institutions must ensure, within the outsourcing agreement of critical or important functions with the service provider, that the service provider provides the institution, its external auditors and other persons it appoints for this purpose and the CBK as the resolution/closure authorities of the institutions determined under the legislation regulating this area, with the following:

   2.1. timely and full access to business premises, including equipment, systems, networks, information and data used to provide the outsourcing function, including relevant financial information, personnel and external auditors of the service provider; and

   2.2. Conducting audits or reviews of a part of the service provider's operation that is or may be related to outsourcing, as well as reviews of the performance of outsourced functions that are the subject of the agreement with the service provider, to enable them to monitor the contractual agreement and to ensure compliance with all applicable regulatory and contractual requirements.

3. The FI should ensure, within the contractual agreement with the service provider, that its internal audit function is able to review the contracted function, using a risk-based approach.

4. Institutions should exercise their access and audit rights referred to in this article and determine the frequency of audits and the areas to be audited, using a risk-based approach.

5. For the purpose of conducting the audits and reviews referred to in paragraph 2, subparagraph 2.2, of this Article, an institution may use:

   5.1. joint audits organized, together with other clients of the same service provider and carried out by the institution and these clients or by a third party appointed by them; and

   5.2. third-party certifications and third-party or internal audit reports made available by the service provider.

6. For the outsourcing of critical or important functions, an institution shall assess whether third-party certifications and reports, as referred to in paragraph 5, subparagraph 5.2, of this Article, are appropriate and sufficient to conduct appropriate audits and reviews of the outsourcing arrangements and shall not rely solely on these reports over time.

7. When the contractual agreement carries a high level of technical complexity, for example in the case of contracting services in the 'Cloud', an institution should verify:

   7.1. whether the persons referred to in paragraph 5 of this Article who carry out the audit and/or assessment have appropriate and relevant skills and knowledge to carry out the relevant audits and/or assessments effectively; and

   7.2. whether the staff of the institution reviewing the certifications and/or reports from the persons referred to in paragraph 5 of this article have appropriate and relevant skills and knowledge to conduct relevant audits and/or reviews effectively.

Article 58
Supervision of outsourced functions

1. The FI should monitor, on an ongoing basis, the performance of service providers in relation to all outsourcing arrangements on a risk-based approach and with a primary focus on outsourcing critical or important functions, including ensuring the availability, integrity and security of data and information. Where the risk, nature or scale of an outsourced function has materially changed, institutions should reassess the criticality or importance of that function in accordance with Article 6 of this Regulation.
2. The FI must demonstrate skills, due care when monitoring and managing contracted agreements.
3. The FI should regularly update the risk assessment and periodically report to the management body on the risks identified in relation to the outsourcing of critical or important functions.
4. FIs should ensure, on an ongoing basis, that contracted arrangements, with a primary focus on contracting out critical or important functions, meet appropriate performance and quality standards in accordance with their policies, by:

   4.1. ensuring that they receive appropriate reports from service providers;

   4.2. assess the performance of service providers, using tools such as key performance indicators, key control indicators, service delivery reports, self-certification and independent reviews; and

   4.3. reviewed all other relevant information received from the service provider, including reports on business continuity measures and testing.

5. FIs should take appropriate action if they identify deficiencies in the provision of a contracted function. In particular, institutions should follow up on any indicators that service providers may not be performing the contracted critical or important function effectively or in compliance with applicable laws and regulatory requirements. If deficiencies are identified, financial institutions should take appropriate corrective or remedial action. Such action may include terminating the contracted agreement, with immediate effect, if necessary.

Article 59
Supplier competence

The FI should only enter into contracts with suppliers who demonstrate high competence and qualified personnel for the delegated functions and effective Technological Risk Management (TRM).

Article 60
Cloud Computing

1. The CBK should be notified of plans to enter into contracts with Cloud Service Providers (CSP) for the provision or material support of critical services, with sufficient notice (one month) prior to the engagement, to allow the supervisor to conduct a risk assessment and raise concerns, if any.
2. The use of Cloud-based services for critical services/functions must be approved by the board, and a register of all Cloud services used by the FI for business functions must be available at all times.
3. The Board and the FI must understand and fulfil their responsibilities regarding the security of the Cloud resources under their control ("Cloud security"), while obtaining independent assurance that there is sufficient commitment and capacity of the CSO regarding the security of the infrastructure of the aforementioned Cloud resources ("Cloud security").
4. The FI must maintain control over the location of financial and personal data stored and processed within the CSO.
5. The storage and processing of financial and personal data in the Cloud should be limited to jurisdictions with relevant laws or international treaties that provide the same level of protection for financial and personal data as domestic legislation.
6. The FI should require the CSO to obtain a no-objection statement before subcontracting parts of the contracted service.
7. The FI should require the CSO to ensure strict logical separation of its virtualized data and resources from other CSO users.
8. Termination policies should provide for an orderly exit and transfer of data if the FI or the Cloud service provider wishes to terminate the contract.

CHAPTER X

ARTIFICIAL INTELLIGENCE

Article 61
Development and deployment of solutions enabled by Artificial Intelligence

1. The FI should establish an Artificial Intelligence (AI) governance framework to oversee the use of AI.
2. FIs should align the development and deployment of AI with their strategic objectives, ethical guidelines, and risk management policies.

3. Boards of directors should ensure that AI systems are compliant with regulatory requirements and within their risk appetite. FIs should ensure board-level awareness and accountability for the deployment of artificial intelligence.
4. The FI should conduct comprehensive risk assessments for AI systems, including operational, financial, reputational and legal risks.
5. FIs should ensure that AI systems are free from bias, adhere to the principles of fair treatment and do not lead to discriminatory outcomes. AI models should be documented, ensuring that they are explainable and auditable.
6. AI systems used in critical functions should undergo stress testing to assess their performance under different conditions.
7. The FI must ensure that the data used in AI systems is accurate, complete and free from bias.
8. The FI must validate AI models before deployment and regularly thereafter.
9. The FI should ensure that AI systems are interpretable for internal stakeholders and, where applicable, for clients.
10. The FI should notify customers when AI is used in decisions that affect them (e.g., loan approvals, risk profiling). Channels should be provided for customers to appeal AI-supported decisions.
11. The FI must immediately report incidents involving AI malfunctions, violations or negative results.
12. FI must adhere to the principles of fairness, accountability, transparency, and human-centered design.
13. Implementing AI-enabled solutions in critical functions should require prior regulatory approval.

CHAPTER XI
FINAL TRANSITIONAL PROVISIONS

Article 62
Enforcement, remedial measures and administrative penalties

Any violation of the provisions of this regulation shall be subject to corrective measures, administrative penalties and monetary sanctions as set out in Law No. 03/L-209 on the Central Bank of the Republic of Kosovo, as amended and supplemented by Law No. 05/L–150, Law No. 04/L-093 on Banks, Microfinance Institutions and Non-Banking Financial Institutions, Law No. 04/L-155 on the Payment System, Law No. 05/L-045 on Insurances, Law No. 04/L-101 on Pension Funds of Kosovo, as well as Law No. 04/L-018 on Compulsory Motor Liability Insurance.

Article 63
Applicability

This Regulation shall prevail over all provisions of the CBK's normative sub-legal acts regulating information systems and cyber risk management of financial institutions that are not in accordance with this Regulation.

Article 64
Annexes

1. The following annexes are an integral part of this regulation:
   1.1. Annex 1 – Immediate Information Reporting Template
   1.2. Annex 2 - Detailed Incident Report Template.
2. Annex 1 - Immediate Information Reporting Template and Annex 2 - Detailed Incident Report Template contain minimum definitions and requirements. They may be supplemented and replaced by specific instructions issued by the CBK.

Article 65
Guidelines

For the purposes of implementing this Regulation, the CBK shall issue specific instructions.

Article 66
Abrogation

1. Upon the entry into force of this Regulation, the following provisions are repealed:
   1.1. Regulation on Information Technology for Banks;
   1.2. Regulation on Systems and Information Security for Pension Funds;
   1.3. Article 7 - Server room requirements, from: Regulation on Minimum Security Requirements
   1.4. Article 3, paragraph 2.d, from: Regulation on the Delegation of Functions of Insurers.

Article 67
Entry into force

This Regulation enters into force on 15 September 2025. Financial institutions - FIs are obliged to comply with the requirements of this Regulation, from 1 June 2026.

Dr. Sc. Bashkim Nurboja,
Chairperson of the Board of the Central Bank of the Republic of Kosovo.

ANNEX 1 - IMMEDIATE INFORMATION REPORTING TEMPLATE

	IMMEDIATE INFORMATION REPORT
Notes:	
a	The incident must be reported within 4 hours of its identification. A second report in the prescribed format must be provided after the initial investigation, within 72 hours of the occurrence. Updates must be provided whenever any developments occur until the submission of the closure report.
b	The incident report should be sent to the Information Systems Supervision Division at dmsi@bqk-kos.org
c	The report should be preceded by an immediate telephone conversation with CBK officials (while the report is being prepared).
d	The report must be signed by the CISO.
Basic information	
1	Name and address of the reporting bank
2	Names of two high-level contacts. Include phone numbers and email addresses.
Incident summary	
1	Nature of the incident (e.g., DDOS, ransomware, data breach/theft, website cloning or defacement)
2	Brief description of the incident
3	Time of incident and time of discovery
4	Affected systems (e.g., CBS, Treasury, trade finance, online banking, ATMs, payment systems such as SWIFT, RTGS, ACH), indicating whether the affected systems are critical or non-critical.
Reporting details	
1	Date and time of reporting to supervisor/other authorities
2	Name of the person reporting
3	CISO name and contact details (at least two phone numbers and emails)
Immediate knowledge of the cause of the incident	
1	Brief description of what caused the attack to succeed
Impact of the incident	
1	Expected disruption of critical systems affecting customer transactions and payment systems
2	The extent and nature of the data breach
3	Financial impact in terms of stolen money, disrupted business transactions, etc.
4	The availability of technical staff to handle the situation and whether all designated staff are present. If not, list alternative arrangements that have been made, including contracted staff.
Corrective measures taken	
1	Temporary measures to mitigate/solve the problem and the reasons for taking such measures
2	Measures taken to protect data and other details necessary for a forensic audit
3	Steps taken/to be taken to clean the system from further damage
4	Proposed steps to prevent further recurrence of this damage
Media and stakeholder management	

1	Any communications with the media and various stakeholders/authorities (e.g., cyber police). A copy of such communications should be attached.
2	If communication documents have not been collected, provide the reasons why they have not been collected and the next steps in this regard.
CISO signature	
Name and contact details - two phone numbers, email address	

ANNEX 2 - DETAILED INCIDENT REPORT TEMPLATE

	DETAILED INCIDENT REPORT
Bank name and address	
Reference details	
1	Reference number and date of the Immediate Information Report (IIR) submitted
2	Nature of the incident reported in the IIR
3	Update number and date of this report
Contact information:	
1	Name of the person reporting and signing the report
	Function
	Contact phone numbers (at least two)
	Email address of the reporting person
2	Name of alternate reporting person
	Function
	Contact phone numbers (at least two)
	Email address of the reporting person
3	Name of the person who submitted the baseline report
	Function
	Contact phone numbers (at least two)
	Email address of the reporting person
	(Correspondence should be sent to the person submitting the report and copied to other contacts. Prompt responses to correspondence are expected.)
Incident details	
1	Severity of the incident (please provide details of the different scales used)
2	Detailed description of the attack
3	Affected customer-facing applications/network
4	How was the attack first detected?
5	Who discovered the attack first?
6	What immediate action was taken to stop the spread or impact of the attack?
7	To what level did the action escalate?
8	The name of the hardware manufacturer, software developer, make/model, etc., of the affected applications, including that of the systems/networks on which the applications run
9	Were the above vendors informed and what was their reaction?
10	Details of the TCP or UDP ports involved in the incident
11	The IP address of the affected system and the attacker, if available
12	Status of action taken to clean the system and resolve issues
13	When can normal business be expected to resume?
14	What arrangements have been made for a follow-up audit?
15	What arrangements are made for an investigative audit?
16	Has the chain of custody been maintained? This includes keeping a detailed record showing who has collected, handled, transferred or analyzed the evidence since the beginning of the investigation.

17	What evidence is seized and kept in secure storage for analysis and as investigative evidence? Evidence may include servers, hard drives, CD-ROMs, emails, images, documents, logs, etc.
18	What investigative tools were used to collect evidence?
19	What vectors were involved in the attack? Provide details on the devices, applications, etc., and what went wrong.
	Equipment: servers, routers, storage devices, IPS, firewalls, VPN, Wi-Fi, Active Directory, IDS, ISAM, mail, DHCP, DNS, endpoints, mobile devices, cloud, SaaS, third-party vendor applications, etc. **Nature of the attack**: password compromise, human intervention, (phishing), social engineering, spam, malware mail, stolen certificates, undiscovered vulnerability, denial of service, zero-day attack, ransomware attack, data theft, etc.
20	IP addresses and domain names to which the attack can be traced
21	Unusual traffic, unusual activity from locations where business is not normally conducted, unusual requests from privileged users and administrators, high number of login attempts, multiple requests for the same file, high volume of data requests, unusual changes to the system, unusual domains, unauthorized settings, configuration changes, etc.