National Bank of Ukraine

Discussion Paper

on the Ethical and Responsible Use of Artificial Intelligence by Participants in the Ukrainian Financial Services Market

Contents

I. Preface

Artificial intelligence (AI) is rapidly transforming the financial sector on a global scale, and – combined with the digitalization of financial services – it is changing financial institutions' business models, approaches to how they do business, and what households and businesses expect from public institutions.

The National Bank of Ukraine (NBU), in fulfilling its mandate to ensure the security and stability of the financial system, protect the interests of depositors and creditors, as well as consumers of banking, non-banking financial, and payment services, and prevent crises, pays particular attention to issues regarding the use of digital technologies, in particular AI, by providers of financial, ancillary, payment, and limited payment services in Ukraine that are subject to the state regulation and supervision by the NBU, which it performs in accordance with the Law of Ukraine *On the National Bank of Ukraine*, the Law of Ukraine *On Financial Services and Finance Companies*, the Law of Ukraine *On Banks and Banking*, the Law of Ukraine *On Insurance*, the Law of Ukraine *On Consumer Lending*, the Law of Ukraine *On Payment Services*, other laws of Ukraine, and NBU regulations (hereinafter referred to as "financial services market participants").

AI opens up significant opportunities for improving process efficiency, managing risks, raising quality of services, and fostering innovation. At the same time, the use of AI may give rise to new types of risks for clients, financial stability, and the transparency of decision-making by financial sector participants, as well as a decline in trust in the financial sector.

Ukraine currently has no adequate legal framework or designated law to govern AI. At the same time, there are strategic documents (the *Concept for the Development of AI in Ukraine*, approved by Ordinance No. 1556 of the Cabinet of Ministers of Ukraine dated 2 December 2020, the *Strategy for Digital Development of Innovative Activities in Ukraine until 2030*, approved by Ordinance of the Cabinet of Ministers of Ukraine No. 1351 dated 31 December 2024), the *Roadmap for AI Regulation*, and the *White Paper on the Regulation of Artificial Intelligence in Ukraine*, published by the Ministry of Digital Transformation of Ukraine on 26 June 2024, which provide for the phased development of regulation and the subsequent formulation of sectoral recommendations to precede laws and other regulatory acts in the field of AI.

It should be noted that, given the path toward European integration, the NBU takes into account the European regulatory model, according to which the horizontal framework in the field of AI in the European Union is established at the cross-sectoral level, specifically within the framework of Regulation (EU) 2024/1689, initiated by the European Commission and adopted by the European Parliament and the Council (EU) on 13 June 2024, which establishes harmonized rules regarding AI (EU AI Act).

A November 2025 survey by the NBU showed that financial services market participants have already been applying AI and machine-learning technologies. A total of 208 financial services market participants took part in the survey. Specifically, 64% of them reported using AI/ML solutions, with 23% indicating active use.

These findings confirms that Ukraine's financial sector is already at a point where practical implementation of AI technology is underway, and that a set of generally accepted guidelines is necessary to ensure the responsible use of AI.

II. Purpose and Scope of the Discussion Paper

The purpose of this discussion paper is to initiate an open, expert discussion with financial services market participants regarding the current and future application of AI technologies in Ukraine's financial sector, aiming at:

- assessing the impact of AI on financial stability as well as on reliability and continuity of financial services
- identifying risks to the protection of consumers of financial, ancillary, payment, and limited payment services (hereinafter "consumers"), including risks of discrimination and non-transparent automated decisions
- ensuring security and stability of the financial system and preventing crises
- identifying regulatory challenges and assessing the adequacy of the current regulatory framework
- developing approaches to the responsible, safe, and ethical use of AI
- collecting proposals for the further development of the NBU's regulatory policy regarding the use of AI, in particular the *White Paper on the Use of AI*.

This discussion paper is addressed to financial services market participants.

The discussion paper is a consultative document intended to inform the subsequent development of policy, regulatory frameworks, or strategies – a white paper in particular – on the use of AI by financial services market participants.

The terms in this discussion paper are used with the following meanings:

automated decision-making refers to making decisions or issuing recommendations using algorithms without direct human involvement at every stage

semi-automated decision-making refers to decision-making or issuing recommendations using algorithms with direct human involvement at every stage. Decisions are not made solely on the basis of results generated by an AI system, but the responsibility for making the decision rests with an authorized representative of the financial services market participant

bias means a distortion in results generated by an AI model that leads to unfair or discriminatory decisions

AI systems are information and communication systems designed to operate with varying levels of autonomy and capable of demonstrating adaptability; based on received input data and a set of human-defined objectives, they can draw conclusions and generate outputs (including predictions, texts, recommendations, or decisions)

AI (Artificial Intelligence) is a general term for a set of information technologies, such as algorithms, methods, approaches, models, and services, involved in the creation and development of intelligent systems capable of performing tasks that typically require human intelligence

AI/ML solutions refer to solutions based on AI/machine learning

Interoperability is the ability of different information systems, devices, software, or components to interact with one another, exchange data, and effectively use that information, regardless of the developer, platform, or location.

Other terms in this discussion paper are used in the meanings defined by Ukrainian laws, regulations, and strategic documents on the implementation of AI in Ukraine.

Questions to discuss:

Question 1. Question 1. In which business areas are you already applying AI technologies, and what types of models do you use (supervised/unsupervised learning, generative AI, etc.)? What are the key drivers for AI adoption in your organization (improved efficiency, cost reduction, regulatory requirements, competitive pressure, better customer experience)? What hidden barriers (organizational, cultural, staffing, technological) are restraining the scaling of AI even when the technology and budget are available?

Question 2. In which processes does your institution use automated or semi-automated AI-based solutions, and what mechanisms of human oversight or intervention are in place at the various stages of the decision-making process? What procedures and frameworks do you use for risk management and for validating models and testing their resilience to changes in input data, particularly in the areas of lending, financial monitoring (AML/CFT), anti-fraud, and transaction monitoring? To what extent, in your opinion, does the current risk-based approach adequately account for the specific risks of automated decisions in the financial sector? What should be considered in the White Paper for the financial sector when applying AI technologies?

Question 3. What key performance indicators (KPIs) do you use to evaluate the effectiveness of AI implementation? Do you conduct a comparative analysis of the quality of decisions made using AI versus traditional approaches? What lessons have you learned from failed or partially successful AI pilot projects?

III. Regulatory Framework to Be Taken into Account by Financial Services Market Participants when Implementing and Using AI

Ukraine's regulatory framework governing the use of AI in the financial sector can best be described as fragmented, evolving, and still in its formative stages. In other words, there is no specific, comprehensive regulation of AI in the financial sector in Ukraine. The use of AI is regulated indirectly – through existing provisions of financial, civil, information, and regulatory legislation. Approaches to regulating AI are in the conceptual and policy-making stages, taking into account European and international practices.

Therefore, the regulatory framework for the use of AI in the financial sector is currently neither whole nor specialized. Regulation is primarily carried out through general requirements for risk management, consumer protection, and information security, which do not fully account for the specifics of AI technologies. This necessitates the development of the NBU's approaches to the application of AI based on the principles of proportionality, risk-based regulation, and technological neutrality.

When implementing AI systems, financial services market participants should take into account the provisions of international and industry standards in the field of AI governance, such as:

1) Glossary of AI Terms (Ministry of Digital Transformation)

2) White Paper on AI Regulation in Ukraine (vision of the Ministry of Digital Transformation) (consultation version), June 2024

3) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence

4) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector

5) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR)

6) ISO/IEC 22898:2022 Information technology – Artificial intelligence – Artificial intelligence concepts and terminology

7) ISO/IEC 23894:2023 Information technology – Artificial intelligence – Guidance on risk management

8) ISO/IEC 27001:2022 Information technology — Security techniques — Information security management systems — Requirements

9) ISO/IEC 42001:2023 Information technology – Artificial intelligence – Management system

10) AI Risk Management Framework issued by the AI Risk Management Framework National Institute of Standards and Technology (NIST), U.S. Department of Commerce, in January 2023.

Questions to discuss:

Question 1. Does your institution have an internal strategy or policy for the use of AI, and is it aligned with the approaches outlined in the Ministry of Digital Transformation's White Paper on AI Regulation? What are the most critical gaps or inconsistencies you see in the current regulatory approach to AI that affect the implementation of these technologies in your organization? In your opinion, what should be included in the White Paper for the financial sector to ensure the responsible and ethical implementation of AI technologies, taking into account the specifics of financial, ancillary, payment, and limited payment services?

Question 2. Which provisions or approaches from the EU AI Act, the NIST AI Risk Management Framework, ISO/IEC 42001, ISO/IEC 27001, and other international standards do you already apply, either partially or fully, in your operations? Which of the international approaches are most relevant and practically applicable to Ukraine's financial sector, and which require adaptation to the national context, limited resources, or market specifics? In your opinion, what should the approach be to implementing the White Paper's recommendations for the financial sector (phased implementation, voluntary compliance, mandatory requirements for certain categories of institutions)?

Question 3. Do you believe that additional guidance or methodological recommendations from the NBU are needed regarding the application of current legislation (on personal data protection, information security, and consumer protection) in the context of AI use? What specific regulatory issues or “gray areas” cause the most concern when implementing AI solutions?

IV. Key principles for responsible use of AI by financial service market participants

Implementation and use of AI systems by financial service market participants should be based on the following key principles:

1. Legality and regulatory compliance.

Use of AI systems should comply with Ukrainian legislation, NBU regulations, licensing terms, and consumer protection laws in financial, ancillary, payment, and limited payment services, and with international principles for responsible use of AI at every stage of its life cycle.

Participants in the financial services market must meet the requirements for:

- protection of restricted information, personal data, bank secrecy, financial service secrecy, payment service provider secrecy, and insurance secrecy

- authorization of participants in the market for financial, ancillary, payment, and limited payment services, as well as the terms of NBU regulations regarding accounting systems, information systems, and software.

Use of AI should not lead to violation of Ukraine's legal requirements or breach of consumer rights in financial, ancillary, payment, or limited payment services.

2. Feasibility, benefits, and responsible use.

AI systems should be put to functional use based on conscious, reasonable, experimentally tested, thoroughly thought through decisions, with a focus on safe and responsible use.

Functional use of AI:

- should not be formal or experimental
- should focus on safety.

3. Transparency, clarity, and awareness.

Financial services market participants must maintain the right level of transparency when using AI. They specifically should:

- inform customers about the use of AI in products, services, or processes
- explain the role of AI in decision-making without revealing trade secrets or sensitive information
- label public materials created or significantly modified using AI systems.

4. Risk-based approach.

Risk management associated with the use of AI should take into account the context of application and the scale of impact and potential harm.

It is feasible for financial service market participants to:

- categorize AI systems by level of risk (e.g., low, medium, or high as independently defined by financial service market participants given the impact and potential harm that using an AI system could cause them)
- apply proportionate control measures and run tests with human participation and supervision
- integrate AI risks into the overall risk management system (upon relevant changes to laws and regulations).

5. Confidentiality, data protection, and information security.

Use of AI systems should comply with data minimization principles (using only the data necessary and relevant for the specified purpose of AI systems operation) and rules for targeted limitation of data processing and for confidentiality, integrity, and availability of information.

Use of AI solutions must meet the condition that their providers share data in compliance with the Law of Ukraine *On Cloud Services* and the Law of Ukraine *On Information Protection in Information and Communication Systems*, and the condition that clear contractual terms be put in place that:

- define the purposes and limits of data usage
- ban unauthorized model use or model training
- ensure that financial services market participants comply with data security requirements.

6. Ethics, non-discrimination, and inclusivity.

AI systems must not violate human rights and freedoms or create bias, discrimination, or inequality.

Financial services market participants should:

- take measures to identify and minimize bias when using AI
- take into account the impact of AI on different groups of customers, including those with disabilities and other reduced-mobility demographics
- prevent the use of AI for discriminatory, manipulative, or exploitative practices.

7. Human oversight, accountability, and reporting.

Decisions and outcomes generated by AI systems should be subject to proper human oversight (participation and supervision) when they can have legal, financial, or social consequences.

Participants in the financial services market should ensure that:

- responsibilities are divided clearly between AI developers, providers, and users
- humans are able to participate in AI decisions and outcomes
- internal paperwork on AI systems operation is maintained.

8. Rights of clients of financial services market participants.

Clients of financial services market participants should have the right to:

- know when AI plays a significant role in decisions that affect them
- receive explanations regarding such decisions
- request reviews and appeals of automated decisions.

9. Adaptability, reliability, and operational resilience.

AI systems should be regularly reviewed, tested, and kept up to date with:

- technology development
- changes in risk profile
- regulatory environment.

Financial services market participants should have procedures in place to suspend, adjust, or decommission AI systems if unacceptable risks or harm are identified.

10. Integration and responsible scaling.

AI systems should be used as coherent parts of the IT, operational, and management architecture and should come with an option to safely expand their use without losing control, quality, security, or compliance with ethical principles.

It is feasible that financial services market participants ensure that AI systems:

- are integrated into existing processes, IT architecture, and risk management, internal control, and compliance systems and do not operate in isolation
- do not violate the interoperability of IT systems and are compatible with existing IT architecture
- are scaled in a controlled manner whereby expansion of AI functionality, number of users, or areas of application is carried out in stages and with full awareness of the risks.

Questions to discuss:

Q1. What principles of responsible use of AI do you consider to be the most critical and fundamental to the financial sector? Which of the principles defined in international approaches (EU AI Act, OECD AI Principles) or in the ICC White Paper are the hardest to implement in your institution? Why are they difficult (resource limitations, technical challenges, logistical barriers?) How should the regulator ensure compliance with these principles: through requirements, recommendations, supervisory expectations, or by encouraging voluntary initiatives?

Q2. Do any of the principles laid out in this document require additional regulatory clarification and/or examples of best practices in their standardized application? If so, please indicate the relevant line of business, such as lending, AML, anti-fraud, transaction monitoring, etc., the nature of the regulatory uncertainty, the approach taken by the institution, and the types of clarifications or examples of best practices.

V. Risk-based management and AI management systems

The NBU expects financial services market participants to ensure that AI management systems are implemented as components of overall corporate governance, risk management, and internal control systems (upon relevant amendments to laws and regulations). The NBU also expects that financial services market participants will pay due attention to information security and cyber protection at every stage of the AI life cycle and make sure there is no deterioration in the level of information security and cyber protection as a result of implementing AI systems.

AI management systems should guarantee that:
1) use of AI systems is responsible, safe, and ethical
2) AI decision-making is based on accountability and transparency
3) management and control measures are proportional to the level of risk
4) proper management is exercised throughout the life cycle of AI systems.

An AI management system should cover all stages of AI systems' lifecycles, including:
1) initiating and deciding on the use of AI:
2) design and development or acquisition and integration
3) testing and validation
4) implementation and operation
5) review and update
6) decommissioning
7) saving decision history and data.

The NBU expects financial services market participants to manage AI systems taking into account the risks associated with:
1) nature of automated or semi-automated solutions
2) relevant model risk
3) scale and duration of the impact of such decisions on customers
4) possible consequences for the rights and legitimate interests of clients
5) potential impact on financial stability and operational resilience.

AI systems should be categorized by risk level (low, medium, high). The level of management, control, testing, and human oversight should match the identified level of risk.

For high-risk applications, particularly in lending, AML/CFT, fraud prevention, and automated decision-making, an enhanced level of management and control is expected.

The NBU recommends that financial services market participants have a clear division of roles and responsibilities in the use of AI. Specifically:

1) The management bodies of financial services market participants should be involved in determining the principles and approaches to the use of AI, and the financial institution's units should report to the management bodies about the use of AI.
2) Specific officials or units should be put in charge of the operation and performance of AI systems.
3) It is feasible to correctly separate the functions of developing, using, and controlling AI systems.
4) Responsibility for decisions made using AI cannot be shifted over to the algorithm or technology provider.

Financial services market participants should implement control mechanisms that promote confidence in the use of AI systems, in particular by:
1) following internal procedures for assessing the compliance of AI systems with established principles
2) running regular (e.g. quarterly) tests of the accuracy, reliability, and fairness of results
3) carrying out independent verification of high-risk systems for compliance with established and declared principles for responsible and safe use of AI and with the defined purpose of application
4) documenting the functioning of AI systems and key management decisions regarding them
5) generating internal reports on AI usage results and incidents.

The level of such mechanisms should be proportional to the level of risk and undergo revision if the conditions for using AI systems change.

Financial services market participants should consider their AI management system as a continuous process and:
1) regularly (e.g. quarterly) review approaches to managing AI systems
2) adapt them to technological developments and changes in risk profiles and the regulatory environment
3) be ready to interact with the NBU within the framework of supervisory activities, consultations, and pilot initiatives.

This approach is consistent with the risk-based logic enshrined in the EU AI Act, as well as the principles of system management defined by the ISO/IEC 42001:2023 standard.

Questions to discuss:

Question 1. Does your institution take a systematic approach to categorizing AI systems by level of risk? What criteria and methodology do you apply to determine the urgency or risk of AI applications (impact on customer rights, financial implications, scale of use, degree of automation, etc.)? How appropriate and applicable do you think it would be to introduce a regulatory categorization of AI systems in the financial sector the way it is done in the EU AI Act (unacceptable risk, high risk, limited risk, minimal risk)?

Question 2. Please describe the key benefits for operational efficiency, service quality, risk management, or customer experience that you expect to gain or have already gained from the use of AI. What risks do you consider to be the most critical in the application of AI in the financial sector (model bias, operational failures, cyber risks, regulatory non-compliance, reputational losses)? What specific measures do you use to identify, assess, and mitigate these risks? How well does your existing model-related risk management framework meet the specific needs of AI risk management?

Q3. What AI management structure is in place in your institution? How is responsibility distributed across functions (business units, IT, compliance, risk management, internal audit) throughout the AI system's lifecycle? What regular checks are carried out to monitor the performance of AI models? What elements of the regulatory infrastructure do you think need to be strengthened to implement an effective risk-based approach to AI regulation? What data sources or analytical approaches can support monitoring the effectiveness of AI technology implementation in the financial sector?

VI. Protecting Consumer Rights in Financial, Ancillary, Payment, and Limited Payment Services

AI systems should be used in compliance with the Ukrainian laws on the protection of consumer rights in financial, ancillary, payment, and limited payment services.

The NBU expects that financial services market participants will ensure compliance with Ukrainian laws on the protection of consumer rights in financial, ancillary, payment, and limited payment services when using AI, maintain an appropriate level of transparency, clarity, and provide the possibility for financial services market participants' employees to intervene in decision-making. Additionally, market participants are expected to consider informing consumers about the use of AI systems as a good practice of responsible application of such technologies.

Informing consumers about the use of AI is advisable, particularly when:

1) AI systems are used for automated or semi-automated decision-making that may affect the rights, obligations, or financial liabilities of the consumer and/or the financial services market participant
2) the results produced by AI systems affect the terms and conditions of provision of financial, ancillary, payment, or limited payment services
3) AI is used in processes related to denying, limiting, or modifying access to financial, ancillary, payment, or limited payment services
4) AI systems are used for the collecting, storing, and processing consumers' personal data.

Consumers should be informed:

1) in a clear, accessible, and unambiguous manner
2) without using technical jargon or specialized terminology
3) in a way that does not mislead the consumer about the role of humans and automated systems in decision-making
4) using the communication channel through which the consumer contacted the provider.

At the same time, the level of detail should be sufficient to convey the fact and general nature of AI use without disclosing commercial or sensitive information or internal algorithms.

The NBU expects that financial services market participants, when using AI systems, will provide consumers with explanations, an important element of exercising the consumer's right to information. The explanation of a decision made using AI shall comply with Ukrainian laws. Such an explanation should be understood as providing the consumer with information about:

1) the main factors or criteria that influenced the outcome
2) the role of the automated system in producing the outcome.

Such an explanation should be tailored to the consumer's level of understanding and should not be reduced to a formal or purely technical description of the algorithm.

The explanation for the consumer should be formulated taking into account:

1) the nature of the financial, ancillary, payment, or limited payment service
2) the potential impact of the decision on the consumer's rights and interests
3) the need to protect banking secrecy, financial service secrecy, secrecy of a payment service provider, insurance secrecy, restricted information (including consumer personal data) as defined by Ukrainian law, and the security aspects of the systems.

It should be noted that providing an explanation does not imply disclosure of source code, detailed algorithms, or other information that could pose risks for the security of AI systems or competition. The NBU expects that financial services market participants will consider reviewing decisions made using AI, engaging responsible persons of financial services market participants, as a good practice for protecting consumer rights.

If a decision made using AI has a significant impact on the rights or financial obligations of the consumer and/or a financial services market participant, it is reasonable to provide the possibility of:

1) reviewing such a decision by an authorized employee
2) making a decision that takes into account the consumer's specific circumstances
3) adjusting the result if an error is detected or the model is applied incorrectly.

Financial services market participants are recommended to ensure:

1) clear and accessible channels for consumer inquiries
2) clear information about the procedure for submitting inquiries
3) timely and substantiated feedback on the results of the review
4) compliance with the requirements of the Law of Ukraine O*n Citizens' Appeals*.

Ensuring transparent procedures for communication and review of decisions helps increase consumers' trust in the use of AI in the financial sector.

Questions to discuss:

Question 1. How does your institution determine when informing consumers about the use of AI is mandatory, recommended, or inexpedient? Which communication channels and formats do you use to ensure accessibility and clarity of such information for different types of consumers? What approaches, principles, or minimum requirements for informing consumers should be considered in the White Paper for the financial sector when applying AI technologies?

Question 2. What mechanisms for providing explanations regarding decisions made using AI have been implemented in your institution? How do you find a balance between providing a comprehensive explanation and ensuring it is understandable to consumers without specialized technical knowledge? Does the institution use AI to inform or serve people with disabilities and persons with reduced mobility? Are there any recorded cases of consumer complaints regarding AI-based decisions, and what are the statistics on their resolution? In your opinion, how can the regulator support the development of AI explainability practices without unduly restricting innovation, for example through guidelines, standards, or supervisory expectations?

Question 3. What procedures are in place at your institution for reviewing and appealing decisions made using AI? Who makes the final decision in the event of a conflict between the AI system's findings and a consumer's request for a review? Is an analysis conducted of the reasons for discrepancies between automated decisions and the results of their review? What approaches to organizing human oversight, review, and appeal of decisions taken by AI should be considered in the White Paper?

Question 4. Do you believe that financial services consumers in Ukraine are sufficiently informed about the use of AI in the financial sector? What measures to improve consumers' financial and digital literacy in the context of AI could be helpful?

Question 5. What should be considered in the White Paper for the financial sector regarding the application of AI technologies?

VII. Data and Models: Ethical Requirements

The use of AI systems is inherently linked to the quality of data and the correctness of the models on which automated or semi-automated decisions are based.

The NBU expects that financial services market participants will pay due attention to the ethical aspects of working with AI data and models to prevent unfair, biased, or non-transparent decisions. They are also expected to consider ensuring adequate quality and representativeness of data as one of the key prerequisites for responsible use of AI systems.

Good practice should include, in particular:

1) the use of data that is sufficient in volume, up-to-date, and relevant for the specific purpose of AI application
2) the assessment of data sources in terms of their completeness, reliability, and suitability for the context of use
3) regular (e.g. quarterly) review of datasets, taking into account changes in customer behavior, market conditions, and operational environment.

The NBU emphasizes the need to identify and minimize risks of bias that can arise from:

1) non-representative data samples
2) the use of proxy variables that indirectly reflect sensitive features
3) historical distortions in data.

Financial services market participants should consider implementing data analysis and testing procedures as a good practice to prevent discriminatory or unfair outcomes. These procedures can be formalized in the internal policies of financial services market participants.

The use of AI systems shall comply with the requirements of laws on personal data protection and privacy. The NBU expects financial services market participants to:

1) process personal data in line with the defined purposes and the principles of data minimization
2) take into account Ukrainian laws on personal data protection, as well as the provisions of the EU General Data Protection Regulation (GDPR) where applicable
3) ensure transparency regarding the processing of personal data in processes related to AI use.

The NBU expects financial services market participants to conduct regular testing and validation of AI models at least once a quarter as an integral part of the proper management of such systems. Good practices should include testing models for:

1) identifying potential discrimination or unfair outcomes
2) assessing the impact of models on different customer groups
3) verifying the consistency of results across different use cases.

Financial services market participants are recommended to assess the level of explainability of results produced by AI systems, in particular:

1) the ability to interpret results for internal users
2) the ability to provide a clear explanation to customers when required
3) the adequacy of the chosen methods for explaining the model's complexity and the nature of its application.

The NBU emphasizes the importance of testing AI models under conditions that differ from standard scenarios, including:

1) under changed economic or market conditions
2) in the event of data failures or incompleteness
3) when scaling the use of models.

Such testing helps timely identify deviations and inconsistencies, enhances the reliability of AI systems, and improves the predictive capabilities of their models.

Questions to discuss:

Question 1. What data sources do you use for training and operating AI systems? How do you ensure the lawful use of such sources and evaluate their quality, completeness, representativeness, and absence of bias? Do you conduct regular audits of datasets to identify potential sources of discrimination or distortions? What requirements, principles, or approaches to data management for AI systems should be considered in the White Paper for the financial sector?

Question 2. What methods and instruments do you use to detect, measure, and minimize bias in AI models? What procedures for testing AI models do you apply? What regulatory expectations or recommendations regarding the management of the risks of bias and the testing of AI models should be included in the White Paper?

Question 3. How explainable are the AI models applied at your organization? What trade-offs between model accuracy and explainability do you consider acceptable for different use cases? What approaches to defining requirements for

the explainability of AI models, depending on the level of risk and area of application, should be included in the White Paper?

VIII. Operational and Digital Resilience in AI System Usage

The use of AI systems must align with the operational resilience requirements for financial market participants. The NBU expects financial market participants to treat AI systems as a component of their information, communication and operational infrastructure – one that may introduce additional risks, including, but not limited to, business continuity, process stability, and customer protection.

This approach is consistent with European practices established under the EU Digital Operational Resilience Act (DORA) and supervisory approaches to managing ICT risk (risks associated with the use of information and communication technologies).

The NBU expects financial market participants to integrate AI systems into their broader risk management systems.

Best practices should specifically include:

1) Treating AI systems as important elements of the IT landscape, depending on their role in providing financial, ancillary, payment, or limited payment services
2) Assessing how malfunctions, failures, or inaccuracies in AI systems and models affect business continuity
3) Aligning AI usage with existing business continuity plans and disaster recovery protocols.

The NBU emphasizes that financial market participants must be prepared to respond promptly to incidents involving the use of AI systems and models.

Best practices should specifically include:

1) Integrating AI-related incidents into an overarching IT incident management system
2) Establishing procedures for detecting, classifying, and responding to model failures or anomalous behavior
3) Conducting impact assessments of such incidents on customers, financial transactions, and the institution's reputation
4) Ensuring timely customer notification in the event that failures or anomalous model behaviors are identified.

Financial market participants are encouraged to ensure they have the capability to promptly suspend or restrict the use of AI systems and models should a significant incident occur.

The NBU expects financial market participants to view the testing of AI systems' operational resilience as an element of sound AI system management. Best practices in this area should include:

1) Testing AI systems under high-load conditions
2) Verifying model behavior in the event of partial data or IT resource unavailability
3) Simulating failure and disruption scenarios that could impact critical processes.

The level and frequency of such testing should be determined by taking into account the role of the AI system and its potential impact on the institution's operations, informed by IA system performance reviews conducted, preferably, on a quarterly basis.

The NBU expects financial market participants to pay due attention to risks associated with the use of third-party AI systems, particularly cloud-based or platform solutions. Best practices in this area should include:

1) Assessing the criticality of AI solution providers to operational resilience
2) Incorporating requirements for continuity, availability, and security into contractual terms
3) Ensuring there is the capability to monitor or replace a provider as necessary.

In light of the evolving regulatory landscape, the NBU expects financial market participants to:

1) Review their AI utilization strategies in accordance with digital operational resilience requirements
2) Adapt internal policies and procedures as regulatory requirements are updated
3) Maintain readiness for supervisory engagement on matters of operational and digital resilience.

Questions to be discussed

Question 1. Which external AI services, providers, or cloud platforms do you use, and what risks arise from such dependencies? What approaches do you employ to assess, monitor, and control the compliance and security of third-party models? What challenges arise when interacting with AI providers operating across various jurisdictions? In your view, does the regulatory approach outlined in the White Paper drawn up by the Ministry of Digital Transformation require further detail in the Financial Sector White Paper regarding the management of such risks?

Question 2. Which areas of your operations are most dependent on AI technologies, and what potential risks does this create? Are AI systems included in your institution's registry of critical ICT assets? Does your institution conduct assessments of the financial consequences of potential failures, errors, or the misuse of AI models? Which regulatory changes or AI initiatives do you consider most vital and relevant for strengthening your institution's operational

resilience? What are the most critical gaps or uncertainties in current AI regulatory approaches that require priority resolution and inclusion in the Financial Sector White Paper?

IX. Organizational Culture and Competencies

The ethical and responsible use of AI systems depends significantly on staff awareness, organizational culture, and the level of leadership engagement within financial market participants.

The NBU encourages financial market participants to:

1) Invest in upskilling and raising staff awareness regarding the capabilities, limitations, and risks of AI systems, particularly through training, internal communications, and the sharing of best practices

2) Foster a culture of responsible technology use, where ethical considerations, consumer protection, and risk management are viewed as integral components of innovation

3) Ensure proper oversight from senior management, which involves supporting the principles of responsible AI use at executive levels, integrating these principles into the institution's strategy and policies, and ensuring leadership is directly involved in key decisions regarding AI applications.

Fostering an appropriate organizational culture helps mitigate the risks of official or unregulated AI usage and enhances the trust of customers and stakeholders.

Questions to be discussed:

Question 1. How aware is your staff of the principles behind AI model operations, and what training or professional development programs are currently in place? What internal standards do you use regarding model explainability, transparency, and independent validation? Is your institution prepared to provide auditors or regulators with sufficient information regarding the logic and functioning of your models? What requirements or recommendations for staff competency development and internal standards should be prioritized in the Financial Sector White Paper?

Question 2. What challenges do you face in attracting and retaining qualified specialists in AI, data analysis, and machine learning? Are you considering partnerships with universities, research centers, or technology companies to help develop these competencies?

Question 3. How is a culture of responsible AI use being fostered within your institution? Are there mechanisms in place to encourage employees to identify and report potential ethical issues, biases, or AI-related risks? Which principles, tools, or organizational measures would be most effective to include in the White Paper to help create a culture of responsible AI use across financial institutions?

Question 4. Are your institution's governing bodies (Supervisory Board, Management Board) involved in defining your AI strategy and overseeing its implementation? What is the frequency and format of reporting AI usage, associated risks, and incidents to these bodies? In your view, should the regulator mandate the appointment of a Chief AI Officer within financial institutions?

X. Self-Assessment and Continuous Improvement

The NBU expects financial market participants to view the use of AI systems as a dynamic process that requires regular review (e.g., quarterly) and refinement. Financial market participants are encouraged to:

1) Conduct periodic self-assessments of their AI usage practices, taking into account the nature, scale, and risks of specific AI applications
2) Revise internal approaches, policies, and procedures whenever AI usage conditions change or when new risks and incidents emerge
3) Account for technological advancements and the evolving regulatory landscape, including updates to international standards and supervisory approaches, when further utilizing or scaling AI systems.

Regular self-assessment – conducted quarterly, for instance – and a focus on continuous improvements help increase the maturity of AI usage practices, mitigate risks, and ensure alignment with regulatory expectations and the needs of consumers of financial, ancillary, payment, and limited payment services.

Questions to be discussed

Question 1. What key regulatory, technical, organizational, or resource constraints are most hindering the effective and secure use of AI in your institution? What additional resources, data, tools, methodologies, or forms of regulatory support do you require to scale AI applications, ensure proper model explainability, and manage risks effectively? What specific challenges do institutions operating in multiple jurisdictions or engaging in cross-border activities face, and what approaches or mechanisms would best support international regulatory alignment and recognition? Specifically, what should the Financial Sector White Paper include to effectively eliminate existing barriers, enhance interoperability and alignment of regulatory requirements across jurisdictions, and ensure the consistent, proportionate, and practical implementation of responsible AI management principles?

Question 2. How does your institution track and implement best practices, emerging technologies, and international standards for responsible AI usage? Do you participate in AI industry-wide initiatives, working groups, or forums? Do you see it expedient to establish an industry-wide platform or forum for sharing AI usage experiences, best practices, and challenges among financial market participants? In what capacity could the NBU's involvement provide the most value to this initiative? Which regulatory tools or mechanisms (such as pilot regimes, temporary exemptions, individual consultations) could support the innovative yet responsible rollout of AI in your institution? Would you be interested in participating in an NBU regulatory sandbox to test AI solutions?

Question 3. In your view, to what extent do financial institutions lack regulatory certainty regarding the implementation of frameworks, standards or approaches for the ethical and responsible use of AI technologies? Which elements of this regulatory approach – such as principles, requirements, methodology, or practical application expectations – require the most precise and unified definition? What regulatory benchmarks, clarifications, or instruments (such as transition periods, examples of best practices, or a risk-based approach) should be prioritized in the Financial Sector AI White Paper?

XI. Future Interaction Between Financial Market Participants and the National Bank of Ukraine

The NBU views the process of developing these recommendations as an open and dynamic one, emphasizing the importance of an ongoing dialogue with financial market participants. The practical experience of financial institutions – their perspective on the risks, challenges, and opportunities of AI usage – is vital to drawing up balanced and applicable guidelines.

The development of recommendations for the ethical and responsible use of AI by financial market participants will be carried out in stages and will include:

- Publication of a Discussion Paper on the ethical and responsible use of AI by financial market participants. This will serve as a foundational baseline for establishing a shared understanding of AI usage principles in the financial sector in order to obtain feedback and proposals from financial market participants
- Formulation and release of findings, providing a consolidated regulatory response to the results of the discussion
- Drawing up of a white paper for financial market participants as a comprehensive sectoral document reflecting the established approaches, practices, and expectations of the NBU.

We invite financial market participants to submit proposals and actively participate in consultations during the preparation of these documents. If you have any suggestions or comments regarding this document, please send them to ai@bank.gov.ua. Information regarding future consultations will be published on the National Bank's official resources.