Sound Practices for Responsible Adoption of Artificial Intelligence (AI): Consultation report

Response to Consultation

Bank of Russia

1. **Do you agree with the benefits and risks of AI adoption by financial institutions described in this report? Are there any substantive benefits or risks not covered?**

   The benefits and risks of AI adoption by financial institutions are described in the report sufficiently and are consistent with the current stage of AI development.

   At the same time, in terms of benefits, additional attention could be paid to the practices of financial institutions aimed at enhancing financial inclusion through the use of AI (e.g., by explaining to customers the logic behind AI decision-making in credit scoring) or by introducing specialized AI services that help clarify the terms of complex financial products to clients or make financial services more accessible to individuals with disabilities. It is also worth highlighting risks related to the intentional or unintentional misselling of financial services.

   Additionally:

   In 2025, the Bank of Russia conducted its first comprehensive survey of Russian financial market participants in order to learn how AI is being used and how associated risks are being controlled.

   Regarding the benefits for financial institutions from adopting AI, survey results demonstrated that technology is attractive primarily for its potential to reduce operational costs (over 80% of respondents) and optimize risk management processes (70%). More than 50% expect increased transparency and automation of business processes, as well as a stronger competitive position in the market. A third of respondents plan to use AI to improve customer experience. Overall, institutions that consistently use AI do not tend to believe that it significantly increases their risk profile.

   The risks identified as most likely to materialize and with the highest level of potential damage were reputational and operational risks – 20% and 16% of respondents, respectively (assigned them a medium level of concern when using AI). Another 13% identified the risk of dependence on AI solution providers as high.

2. **Are the sound practices sufficiently comprehensive and clear to enable financial institutions' responsible AI adoption?**

We believe the practices described in the report can significantly contribute to the responsible adoption of AI by financial institutions. We also note that one of the well-known and widely accepted methodologies for describing the lifecycle in the field of advanced analytics is the CRISP-DM methodology. In this regard, we believe it would be useful for the FSB report not only to present a recommended illustrative model, but also to provide an overview of existing standards.

We also propose considering the possibility of supplementing individual practices with proposals regarding strategic oversight, governance, and accountability – see the responses to Questions 3 and 4.

Additionally, we would like to note that the Bank of Russia adheres to a similar approach to promoting the responsible adoption of AI in the financial market, as also reflected in the recommendations of the Bank of Russia's Code of Ethics for Artificial Intelligence in Finance.

3. **Do the sound practices strike an appropriate balance between managing risks relating to all forms of AI, and addressing some of the risks relating to emerging and new complex forms of AI, such as GenAI and agentic AI?**

We believe that the described practices are technologically neutral and can be applied to any type of AI implemented in a financial institution. However, certain types of AI may require increased attention from institutions, for example, through special training for employees when using tools based on generative AI and AI agents (including issues related to agent performance, the required level of human involvement, and the procedure for such intervention). We also recommend paying greater attention to risk management approaches associated with multi-agent AI systems, including cybersecurity risks, to address the risks of new and complex forms of AI.

4. **Are the sound practices sufficiently flexible to accommodate and address newer types of AI and responsible adoption over time?**

The practices provide a fairly comprehensive and flexible description of possible steps for responsible adoption of AI by financial institutions. Areas of particular importance include focus on proportionality, AI risk management throughout the lifecycle of AI solutions, and the need to consider the specific features of each particular AI use case.

At the same time, the report could be expanded with recommendations related to the AI decommissioning phase. We also suggest considering the possibility of supplementing some practices with the following provisions:

Sound Practice 1. Strategic direction and oversight.

We would further propose that financial institutions are recommended to develop and approve provisions on the use of AI in their activities within their strategic documents, and, where necessary, to develop a separate strategy for the development and application of AI in the financial institution.

Sound Practice 2. Governance and accountability.

We propose additionally recommending that specialists in handling complaints from customers and consumer protection are involved in the process of the independent third-line review of AI in the institution, as well as the mechanism of internal cross-functional communication for knowledge and opinion sharing.

Sound Practice 8. Explainability and transparency.

We would further propose recommending to institutions to label information, including images, audio, and video materials, generated through the use of generative AI, in cases where the editing of such information materially alters its content, the application of large generative models is not apparent from the context, or where there is a risk of detriment to clients.

Sound Practice 10. Human oversight.

We propose additionally recommending that institutions ensure the performance of functions carried out with the assistance of AI by employees in cases where the use of AI is temporarily unavailable.

Sound Practice 11. Cyber and ICT risk management.

We would propose the following additional AI risks associated with information security and operational reliability when engaging third-party AI solution providers:

1. Risks associated with data management, arising from the use of “poisoned”, outdated, and/or incorrect datasets for AI model training, entailing a disruption in the functioning of the AI system;

2. Data privacy risks, arising, among other things, from the materialization of security threats to AI technologies, resulting in information being made available to unauthorized persons, as well as infringement of copyright and/or intellectual property rights;

3. Risks of disruption to the functioning of the AI model, arising from the materialization of security threats to AI technologies, resulting in a degradation of the AI system's quality, including AI hallucinations, data drift, and other forms of AI model degradation, leading to incorrect conclusions and decisions by the AI model.

4. Risks of insufficient explainability and/or predictability of AI model actions, arising from the complexity of interpreting the results of AI model execution, leading to incorrect conclusions and decisions by the AI model.

5. Risks related to engaging service providers and/or using open-source components of AI technologies, arising from intentional or negligent actions of service provider employees, as well as the presence of weaknesses and/or vulnerabilities in such components.

6. Risks related to disruption of the institution's operational reliability, arising from intentional or negligent actions directed at the AI system, leading to interruptions in the institution's core business processes.

7. Institutions are recommended to take into account AI information security risks in the following cases:

• when determining the feasibility of developing and/or using AI in individual tasks or business processes as a whole;

• when deciding on the use of specific AI technologies;

• when ensuring information security;

• when carrying out AI risk management.

Sound Practice 12. Third-party AI risk management

We propose additionally recommending that institutions, when engaging third-party providers of AI solutions, pay attention to (and, where necessary, specify in the service contract) issues related to ensuring that the service provided by the supplier complies with legal requirements in respect of the function performed under outsourcing, the management of data used for training AI models, and the confidentiality requirements for information transmitted.

5. **Do the case studies in this report sufficiently highlight how different types of financial institutions can benefit from responsible AI adoption? Are there additional case studies for inclusion in the report? If so, please provide such case studies, particularly for nonbanks.**

The examples illustrate quite comprehensively the importance of the responsible adoption of AI.

6. **Do the case studies in this report provide actionable insights for financial institutions in their responsible AI adoption?**

The examples described in the report are of interest to market participants and regulators from the perspective of sharing experience on the capabilities of AI and its applicability to specific tasks in the activities of institutions.

At the same time, the practical value of the examples could be enhanced by indicating specific metrics or benchmarks that can be used for testing and validation of AI, including in the context of specific AI use cases. For instance, they could be provided either as a supplement to the cases described in the text or in Appendix 3, or as a separate list.

The cases presented in the report illustrate successful experiences. In our view, it would also be beneficial for institutions to examine unsuccessful cases and the reasons for their failure.

7. **Are the definitions in the glossary clear and aligned with industry sound practices, including recent developments in AI?**

The glossary could be enhanced by the inclusion of the concept of multi-agent AI systems.

8. Are there any comments you would like to make on this report? Please fill in.