CENTRE DE DROIT
BANCAIRE ET FINANCIER

Artificial intelligence

FINMA’s expectations in terms of governance and risk management

Par Yannick Caballero Cuevas le 19 December 2024

Banks and financial institutions are increasingly integrating artificial intelligence (AI) into their internal services and processes (see e.g. Jotterand, cdbf.ch/1377). In particular, this use can present operational, legal and reputational risks (see e.g. Levis, cdbf.ch/1380), as well as a growing dependence on third-party suppliers, especially for AI models and *cloud* services. Added to this is the difficulty of assigning clear responsibilities in the event of errors in the AI system or model. The use of AI by banks and financial institutions poses a major supervisory challenge. To this end, FINMA has published guidance 08/2024 on governance and risk management when using AI, in which it describes the lessons learned from its supervision.

All regulated entities must consider the repercussions of the use of AI for their risk profile in the light of the regulatory framework in force, and adapt their governance, risk management and control system (see e.g. de Cannière, cdbf.ch/1376). In addition to data protection issues, FINMA is drawing the attention of supervised entities to the robustness and accuracy of AI models and the need to ensure that the results are correct, explainable and free from bias. It therefore focuses its supervision on seven areas : (i) governance, (ii) risk identification and classification, (iii) data quality, (iv) testing and ongoing monitoring, (v) documentation, (vi) explainability, and (vii) independent verification. Some of these issues are also covered in the European Regulation on AI (AI Act), in particular Articles 9 to 15 AI Act on the requirements for high-risk AI systems.

For FINMA, AI governance is essential. It must be established in the light of the risks identified by the supervised entities. They must clearly define the competences and responsibilities for the development, implementation, supervision and use of AI and lay down requirements for model testing, ancillary system controls, documentation standards and training. When taxable persons acquire third-party AI solutions, they must also determine what data and methods are used and the existence of due diligence on the part of the third-party supplier in particular. In the case of outsourcing, tests and controls must be put in place. In addition, contractual clauses must govern responsibilities and liability issues. In addition, regulated entities must ensure that third parties have the necessary skills and experience. In our view, governance needs to be considered holistically, encompassing risk management, internal and external skills, the allocation of responsibilities, and the legal and contractual framework.

In order to identify and classify risks, taxpayers must determine whether the planned application falls within their definition of AI. This definition must be sufficiently broad, otherwise the risk

inventory will not be exhaustive. Defining what constitutes an AI system or model is already a challenge for taxable persons, in the absence of specific legislation on AI in Swiss law. In our view, the AI Act can serve as a source of inspiration (cf. Caballero Cuevas, cdbf.ch/1382). Next, those subject to regulation are required to classify risks according to their importance, their specificity and the likelihood of the identified risks occurring. The AI act also adopts this risk-based approach (see Caballero Cuevas, cdbf.ch/1390). In addition, taxable persons must define systematic criteria enabling them to identify important AI applications that require special attention.

The quality of the results of AI applications depends, to a large extent, on the quality of the data. Depending on the data used in the various phases, the results may be erroneous, inconsistent, incomplete, unrepresentative, outdated or biased. In their internal guidelines and instructions, tax authorities must therefore lay down requirements aimed at guaranteeing the completeness, correctness and integrity of the data and ensuring that it is available and accessible. In our view, however, this expectation is high when reporting firms use AI systems or models from third-party providers. Moreover, FINMA recognises that reporting entities often have no influence on the underlying data, or even no knowledge of it. In order to comply, reporting firms should, in our view, include contractual clauses to enable them to report to the supplier cases where the quality of the data is compromised, and ensure that the underlying data is corrected. In our opinion, this difficulty does not relieve reporting entities of their responsibility to ensure the quality of input data, which is why it is important to provide internal guidelines on data governance and its use in AI systems.

In order to ensure that the AI system or model is working properly, regular testing and constant monitoring are essential. FINMA assesses whether reporting entities provide for regular checks on the accuracy, robustness and stability of the AI system or model. These tests help to ensure that the application is not biased. FINMA expects performance indicators to be used to assess the extent to which the system achieves the objectives set. Reporting firms must also ensure that changes in input data do not affect the AI model underlying the AI application. In addition, licensees must analyse cases where results have been ignored or modified by users, as these situations may be indicative of a weakness in the system or the AI model. They must therefore monitor AI applications throughout their use.

FINMA emphasises the importance of documentation. Reporting entities must have detailed, recipient-oriented documentation (e.g. for advisors, secretaries, *compliance officers*, etc.). For major applications, this documentation must cover the purpose of the application, the selection and preparation of data, the choice of model, performance measures, assumptions, limitations, tests and controls and fallback solutions.

If AI systems and models are to be critically evaluated, it is vital that the results can be explained and understood by the staff of banks and financial institutions. This is all the more true when results have to be explained to investors, clients, employees (cf. Hirsch, cdbf.ch/1384), supervisors or auditors. However, FINMA found that the results were often not understood or explained and could not be critically assessed, which poses a problem for ensuring the robustness and accuracy of the AI system or model.

In summary, the guidance 08/2024 informs us about FINMA’s expectations regarding AI. However, many questions remain, in particular about the practical implementation of these expectations by regulated entities. FINMA plans to develop and communicate these

expectations in a transparent manner. That said, regulators wishing to use AI must be proactive in analysing the regulatory framework, identifying and managing risks, and training their staff. In this respect, they should take an interest in international initiatives. One example is ESMA's statement on the use of AI in investment services.

The issues addressed in this commentary will be discussed at the webinar on artificial intelligence scheduled for 21 January 2025, and explored in greater depth as part of the CAS Digital Finance Law.

Reproduction autorisée avec la référence suivante: Yannick Caballero Cuevas, FINMA's expectations in terms of governance and risk management, publié le 19 December 2024 par le Centre de droit bancaire et financier, https://cdbf.ch/en/1392/