HAWK

Whitepaper

The EU AI Act
What It Means for AML and Anti-Fraud Professionals

Contents

AI Regulation Is Coming.
Is Your Financial Institution Ready?

The European Council formally adopted the EU AI Act on May 21, 2024. Commentators have hailed the act as the world's first set of "comprehensive rules for trustworthy AI." European Commission President Ursula von der Leyen even called it "a historic moment."

While both Parliament and Council still have to formally adopt the agreed text of the AI Act before it becomes EU law, there is little doubt that the regulation will make more headlines in the coming months. The act aims to set a legislative framework for a young and dynamic field of innovation. Courts, supervisory authorities, and other regulatory bodies that enforce the AI Act will have to walk a fine line, providing a level playing field for EU-based innovators in the very competitive global AI landscape, while at the same time protecting EU citizens and their fundamental rights against the inherent risk of (uncontrolled) AI use.

This whitepaper kicks off a series on the different aspects of AI regulation. We will take a closer look at the structure and content of the AI Act and its impact on Anti-Money Laundering (AML) and fraud prevention tools used by regulated financial institutions.

> The Artificial Intelligence Act ("AI Act") is one of the most anticipated pieces of regulation of the EU

Reconciling The Impossible The AI Act’s Risk-Based Approach

Comparable to other regulatory frameworks, and the policy proposals by the Financial Action Task Force (FATF), the EU proposes a risk-based approach to regulating AI.

With this approach, EU legislators aim at providing a horizontal framework for the countless use cases of AI in all areas of the economy and society.

The main challenge for the success of such a regulatory proposal will be to reconcile at least partially diverging goals: on one hand, ensuring the protection of fundamental rights of EU citizens against the inherent risk of AI, and on the other hand allowing sufficient room for innovative approaches through and for the use of AI. To this end, the agreement of Council and Parliament promotes so-called “regulatory sandboxes and real-world testing, established by national authorities to develop and train innovative AI before placement on the market.”

> The agreement of Council and Parliament promotes regulatory sandboxes and real-world testing.

More Rules to Follow The AI Act's Impact on Banking Processes

Banks are already successfully using AI in areas like AML compliance and fraud prevention, and the FATF has highlighted the opportunities (and challenges) of AI in the areas of AML and counter-terrorist financing measures (CFT).

Other areas where the role of AI will also increase in the future are customer service and credit scoring. Due to the relevance of financial services in everyday life and the significant impact AI-based decisions can have on the affected citizens of the EU, the European Commission had already signaled early on that the use of AI in financial services and related use cases may be considered "high risk" under the AI Act. However, whether the use of AI in the area of AML and fraud prevention falls in this category still needs to be determined. Initial indications suggest that such use cases might not be considered high risk. The official guidelines for interpretation of the AI Act will provide for clarity in this regard.

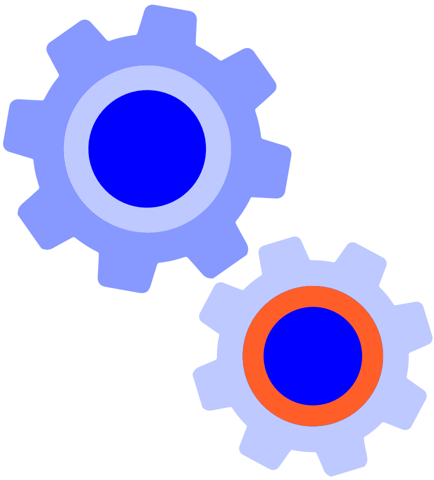
While high risk classifications will come with a higher regulatory burden and stricter obligations, the good news for regulated entities is this: the requirements they will need to fulfil due to the AI Act won't be much different from what regulatory bodies and supervisory authorities such as BaFin or FINMA already expect from their regulated institutions.

> AI Regulation

While the rules for the use of AI come on top of the already existing rules and regulatory technical standards for regulated financial institutions, the governance is similar.

The use of AI in regulated institutions requires adequate internal governance and clear responsibilities. Governance for AI models must include control measures, including adequate risk and outsourcing management.

Ultimately the responsibility for decisions made rests with the company's leadership, i.e., managing directors or the executive board.



Technology and Tools Are Ready The AI Act's Requirements for High-Risk AI Systems

The AI Act stipulates the following requirements for High Risk AI systems in Title III, Chapter 2.

The following is an overview of the requirements and a discussion of how they can be addressed from an operational perspective through (1) explainability of individual AI-based decisions and (2) adequate model governance processes.

Requirements

- Risk Management
- Data and Data Governance
- Technical Documentation and Record-Keeping
- Transparency and Information for Users
- Human Oversight
- Accuracy, Robustness, and Cybersecurity

Further Reading

- EU AI Act: First Regulation on Artificial Intelligence
- Opportunities and Challenges of New Technologies for AML/CFT
- AI Act Enters into Force
- Digital Single Market for Europe
- AI Act Regulatory Framework
- Big Data and Artificial Intelligence: Principles for the Use of Algorithms in Decision-Making
- FINMA Risk Monitor 2023: Current Risks in the Financial Sector

Risk Management

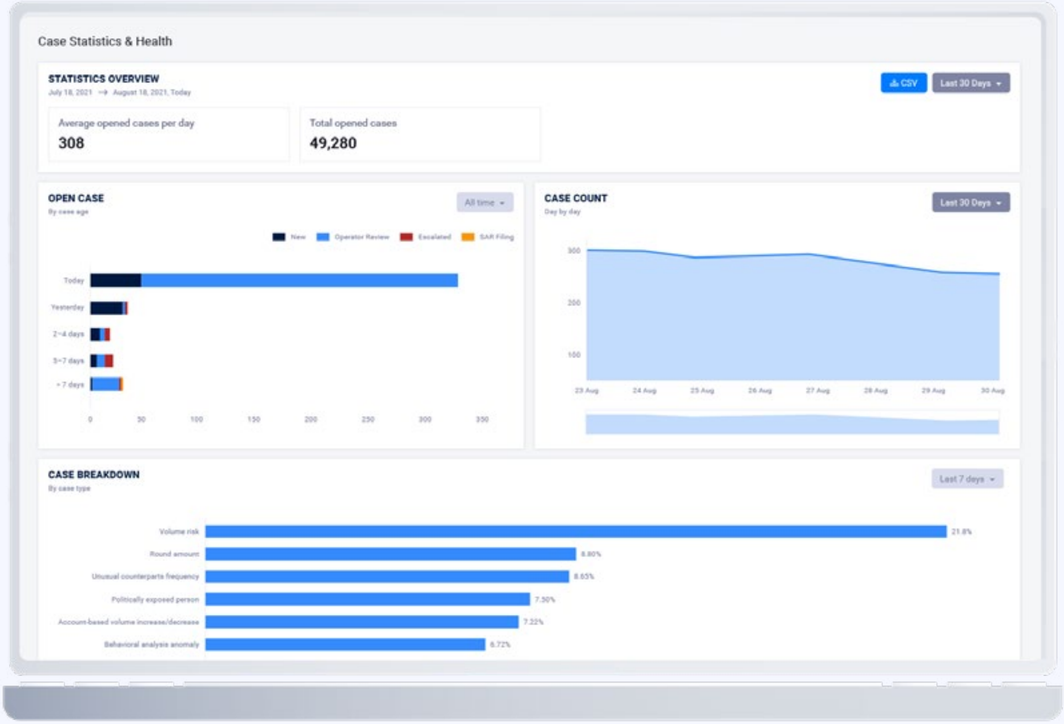
Article 9

The key to addressing the AI-related risk management requirements, aside from a proper risk and business impact analysis, is using a machine learning lifecycle platform such as the open-source platforms MLFlow or Neptune.

These platforms provide full model lineage and traceability. They also provide versioning of models, tracking every step of the training process, including who did what, when they did it, and which data was used to train, test and record every artefact generated from the process.

Such a system allows for quick experimentation and testing, essential in creating effective AI models, automatically creating a full audit trail. The test regime is essential in the risk management requirement and can be done both during model training and during model inference time (runtime).

Testing should look at overall model performance through KPIs alongside looking at individual results through sampling. Such a testing and validation regime is also the foundation for the need of a quality management system (Article 17) for users of high-risk AI systems.



Case Statistics & Health

STATISTICS OVERVIEW

July 18, 2021 → August 18, 2021, Today

Average opened cases per day
308

Total opened cases
49,280

Example of using an experiment tracking tool to compare two different model versions, enabling humans to sign off on a new model before it is activated.

Top: Detected changes in parameters and features between the old and new model version.

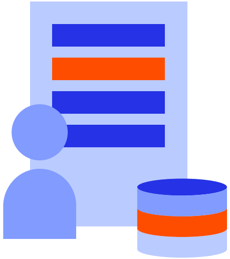
Bottom: Impact of the change on the anomaly score distributions for both 'suspicious accounts' (ie bad actors) and 'normal' accounts.

Data and Data Governance

Article 10

Data quality drives the effectiveness of AI models through training, validation and test data sets.

Practically, that means looking at data using statistical methods, where particular categorical features like customer types need to be cleansed for meaningful input.



Given that large institutions and corporations typically struggle with data quality, we have found that this challenge can be much better addressed within a specific use case. In this context, it's much easier to define defaults for missing values on categorical features.

Another area where special attention is required is the methods of choosing and (sub)sampling of data, making sure that the data sets are representative.

Monitoring and detecting bias or data drifts is also an important part of data management. That can be done with a combination of automatic monitoring of output KPIs, e.g., money laundering alerts above the threshold, as well as building sampling strategies into the model governance process, which will help uncover issues with changes in data.

Technical Documentation and Record-Keeping

Article 11 & 12

Alongside a machine learning lifecycle platform, adjacent documentation on processes and the technical setup of feature generation, training, and model deployment is key.

Record keeping for the model lifecycle is covered by a machine learning lifecycle platform, which provides full audit trail out-of-the-box automatically. At inference time, record keeping is addressed by application audit trail and logging, wherein the AI is embedded alongside the logging, storing explainability results of individual decisions.

Transparency and Information for Users

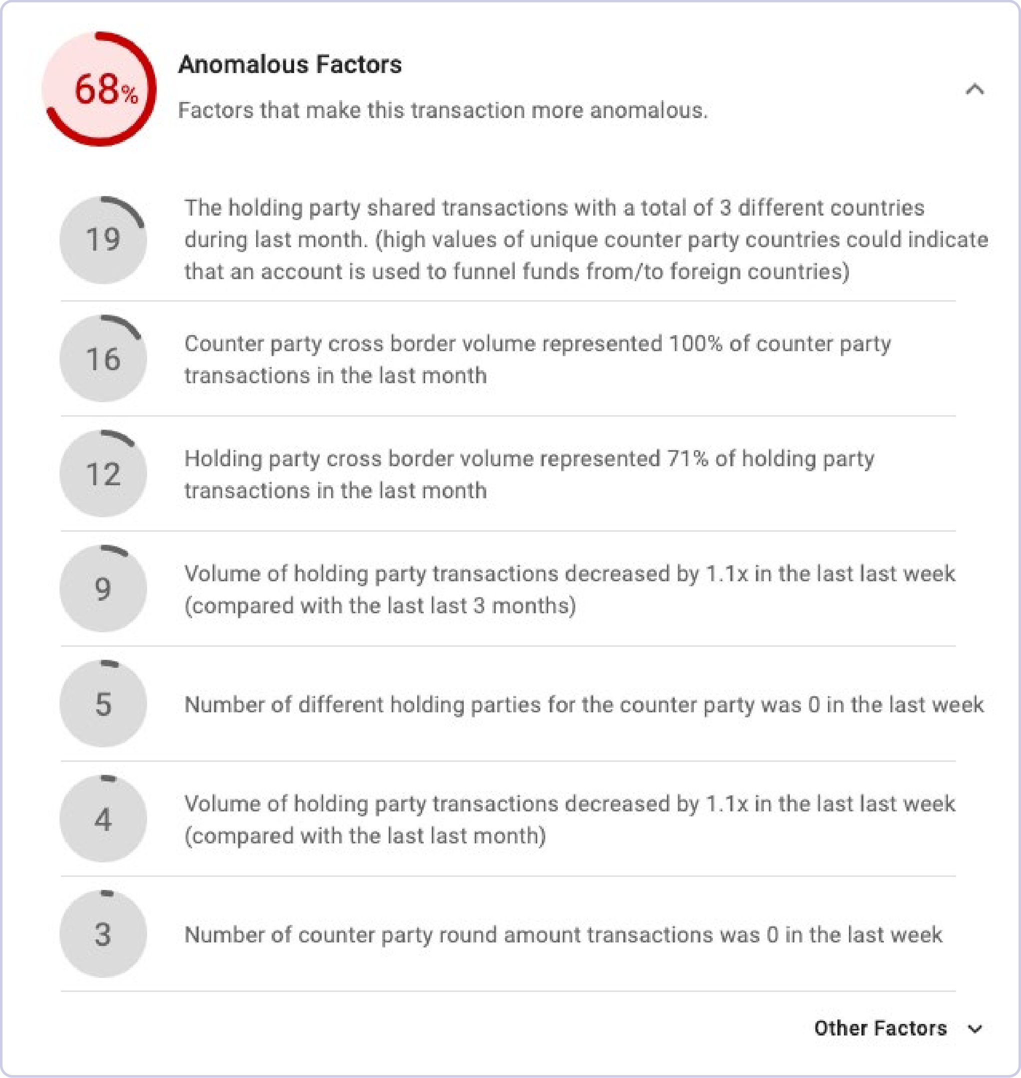
Article 13

Transparency is one of the most crucial elements for trust and acceptance of AI systems.

Every individual AI decision can and should be explainable, recorded with audit trails – including negative decisions. For the use of AI in AML and CFT, explainability must also be provided by the user to the competent authorities to comply with regulatory reporting requirements.

AI explainability is technically possible today, for both classic machine learning models and complex deep learning models. Explainable AI requires clever engineering paired with subject matter expertise. Since it comes with performance application, it should be built into AI-based systems early.

The key to explainability is illustrating the most important decision criteria in human understandable language, supported with values or statistical comparisons, e.g., peer group benchmarking.



68%

Anomalous Factors

Factors that make this transaction more anomalous.

19 The holding party shared transactions with a total of 3 different countries during last month. (high values of unique counter party countries could indicate that an account is used to funnel funds from/to foreign countries)

16 Counter party cross border volume represented 100% of counter party transactions in the last month

12 Holding party cross border volume represented 71% of holding party transactions in the last month

9 Volume of holding party transactions decreased by 1.1x in the last last week (compared with the last last 3 months)

5 Number of different holding parties for the counter party was 0 in the last week

4 Volume of holding party transactions decreased by 1.1x in the last last week (compared with the last last month)

3 Number of counter party round amount transactions was 0 in the last week

Other Factors

Human Oversight

Article 14

Human oversight is key to users trusting AI systems, and hence essential for risk management and model governance.

Here in particular, it's important that humans get control over AI systems, such as the decision on rolling out the initial or new versions of a model.

This control must be based on a transparent model governance process that highlights model output differences based on validating overall KPIs, as well as explainable samples of difference.

Accuracy, Robustness and Cybersecurity

Article 15

Overall model accuracy can be tested during training by looking at classic AI model measures such as AuC (Area under the ROC Curve). Yet model accuracy also needs to be tested on individual results based on sampling.

To guarantee ongoing accuracy feedback loops, samples are required, where sampling can be random but also targeted to edge case through below the line testing, probing results just below a threshold of AI prediction. Automatic above-the-line monitoring of output KPIs, e.g., the number of predicted fraud alerts, helps detect changes in model quality. Automatic monitoring also helps with validating robustness next to necessary runtime redundancy of AI processes.

Conclusion

Explainability and model governance processes are key for the use of AI in banking, AML, fraud prevention, and other areas.

Regulated financial institutions should be well-equipped to implement new or adjust existing risk management processes to address the inherent risks of AI used in their regulated banking processes. If financial institutions also adhere to proper training and technical documentation standards, they can reap the benefits of AI.

For AML and CFT, this means faster and more accurate transactions analysis, significant reductions of false positives and better risk rating results. These efficiency and accuracy gains, as well as providing for the secure and non-discriminatory use of AI technology, are certainly worth the additional effort of implementing the safeguards required by the AI Act and other AI regulations.

> Efficiency and accuracy gains, as well as providing for the secure and non-discriminatory use of AI technology, are certainly worth the additional effort of implementing the safeguards required by the AI Act.

HAWK

Hawk AI GmbH
Friedenstrasse 22B/i3
81671 Munich
Germany

Hawk AI USA Inc
230 Park Ave, Floors 3 & 4
New York, NY 10169
U.S.A.

Hawk AI APAC Pte Ltd
160 Robinson Road, #14-04
Singapore Business Federation Center
068914 Singapore

Follow us on LinkedIn >

✉ info@hawk.ai >

www.hawk.ai >