afme
Finance for Europe

# Building AI for the Financial Sector

## Key Considerations for Vendors

For further information, please contact: Aman Luther – AFME AI Lead (amandeep.luther@afme.eu)

# Contents

## Disclaimer

This document is intended for general information only and is not intended to be and should not be relied upon as being legal, financial, investment, tax, regulatory business or other professional advice. AFME doesn't represent or warrant that the Report is accurate, suitable or complete and none of AFME, or its respective employees shall have any liability arising from, or relating to, the use of this Report or its contents.

## Executive Summary

Financial Services regulations, eg. the EU's Digital Operations Resilience Act, obligate Financial Institutions (FIs) operating within the EU and UK to ensure that third-party technology vendor risks are identified and managed appropriately.

This paper aims to highlight some of the key themes emerging in 2025 relating to GenAI, with the aim of raising awareness of FI's obligations, so that vendors can make adequate provisions and enable FIs to meet their regulatory obligations.

The paper makes 8 key recommendations for vendors:

- Decouple AI features from unrelated releases
- Clearly disclose GenAI functionality
- Give adequate notice of planned AI releases
- Include the ability to "toggle" AI Functionality
- Disclose internal and supply chain use of AI
- Disclose how FI's data is used
- Refrain from "AI washing"
- Provide transparency of Model Architecture

# Introduction

Financial Institutions (FI's) are bound by regulations, including the EU Digital Operations Resilience Act (DORA) (notably, Chapter II: ICT Risk Management, Arts 6 - 14, and Chapter V: Managing of ICT third-party risk. Arts 28 – 30) to ensure that any new tech vendor or product release being must pass through a detailed due diligence and risk assessment process where the product and features are assessed in detail prior to deployment. Not conducting this exercise can have serious regulatory and financial implications on firms and Senior Management and hence is of vital relevance to tech vendors aiming to work with FIs.

In recent months, the growth of functionality afforded by GenAI technology has meant that additional "GenAI Risk Assessments" now must be completed, in addition to existing vendor due diligence, before deployment can occur. It should be noted that this process has to be performed irrespective of how minor the AI functionality may be relative to the wider product. The fact that GenAI it is part of the product, would require an FI client to engage in the due diligence and risk assessment checks described above, before the release can be accepted.

This document has been written with input from several global banks who are AFME members and is an aggregation their collective knowledge. It aims to provide a set of recommendations to technology vendors, to ensure that FI's can meet their regulatory obligations for third party vendor risk management of GenAI.

## Definition of "AI"

For the purpose of this paper AFME applies the EU AI Act's definition of "AI" as below:

*"'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*."

While "GenAI" refers to "Generative AI" which are AI systems capable of generating new, synthetic data like text, images, audio, or video, rather than simply analysing existing data.

# Recommendations

## Decouple AI Features from Unrelated Releases

In some cases, the “AI” component is part of a wider release including other “non-AI” related features. These “all-or-nothing” releases would be at risk of being blocked until the AI elements are risk assessed, irrespective of how minor the AI element is relative to the wider release. It is, therefore, preferable for “AI” components to be decoupled where possible and deployed as stand-alone releases to avoid unnecessary delays to unrelated components.

## Clear disclosure of GenAI Functionality

FIs are increasingly seeing vendors adding “AI features” to their products without prior consultation. While vendors may view these as positive product enhancements, to FIs these are features that cannot be deployed until an AI Risk Review process is completed. FIs require clear disclosure of the use of any GenAI functionality within the product, even if the use is minor. Therefore, clear documentation of the functionality of any release is required, providing as much detail as possible on the GenAI functionality.

## Adequate Notice of Planned AI Releases

FIs have also reported that notification of deployment schedules can often be too late or lacking sufficient clarity. As discussed, while clients in other industries may not have these constraints, FI must perform a risk assessment on every release. Late notification of an AI element can result in a release being declined or temporarily blocked while an AI risk assessment is completed.

As a result, it is recommended that as much notice as possible is provided to clients, alongside detailed documentation, to allow time for the assessment to be completed and not jeopardise any planned release date.

## Include the ability to “toggle” AI Functionality

FI’s would request that wherever possible, vendors should include the ability to “toggle” AI functionality on and off at a user or group. This can ensure that the FI can conduct a controlled release across their estate as deemed necessary and ensure that authorised roles are permitted to use the AI functionality. Often the ability to control a release would make a positive contribution to an AI risk assessment and decrease the likelihood of a release being declined.

## Disclosing Subcontracting and Vendor’s own use of AI

Often it is clear where a firm is entering into a relationship with a vendor who uses AI. E.g. where AI it is explicitly part of the service being purchased. However, FIs are required to risk assess their supply chains and hence vendor use of AI in their own processes and supply chains is also required to be disclosed. This would apply to service vendors as well as technology vendors e.g., a law firm using an AI system for document drafting, or a back-office vendor automating previously manual processes using AI. While the existence of AI within the supply chain would not prevent an FI from using a vendor, disclosure of the use of AI is essential for FIs to fulfil their regulatory obligations for supply chain due diligence and risk assessment.

## Clear Disclosure of the use of FI data and metadata

FI’s require clear disclosure of the use of any data, including metadata or derived data, originating from the FI, including what is stored, where it is stored, what it is used for e.g. training models or product improvement, who has access to it at each stage and when and is maintained or destroyed.

## “AI Washing

“AI washing” is a term describing occurrences when vendors’ marketing may imply a greater use of AI than exists, often with the aim of driving sales / brand value etc. In such circumstances, stating that a product “uses AI” would render FIs duty-bound to conduct a resource intensive AI Risk Assessment to ensure regulatory compliance. This can result in unnecessary delays in deployment of software and hence is a practice that FIs would discourage firms from engaging in.

## Transparency of Model Architecture

Model evaluations are heavily reliant on disclosures by vendors with regards to model architecture, data and training processes. Vendors are requested participate as transparently as is possible to ensure efficient processing of AI risk assessments.

## Conclusion

The integration of AI within the financial sector presents both significant opportunities and challenges. Financial Institutions (FIs) have invested heavily in AI to enhance their processes and offerings to clients. However, the regulatory landscape within the EU and UK necessitates rigorous due diligence and risk assessments for any AI-related functionality introduced by third-party vendors.

Vendors should therefore adhere to the 8 recommendations proposed:

- **Decouple AI features from unrelated releases** – so that releases of other functionality is not impacted
- **Clearly disclose GenAI functionality** – so that AI risk assessments can be performed
- **Give adequate notice of planned AI releases** – to avoid releases being declined due to incomplete AI risk assessments
- **Include the ability to "toggle" AI Functionality** – to decrease the risk profile of a release. This benefits both FIs and vendors.
- **Disclose internal and supply chain use of AI** – so that complete due diligence can be carried out
- **Disclose how FI's data is used** – transparency and trust is essential when working with FIs.
- **Refrain from "AI washing"** – to avoid obligating clients to have to perform time consuming AI risk assessments when not necessary
- **Provide transparency of Model Architecture** – to enable FIs to complete AI risk assessments

By following these guidelines, vendors can facilitate smoother collaborations with FIs, ensuring that AI deployments are both compliant and beneficial to all parties involved. The proactive management of AI risks will not only enhance the trust between FIs and vendors but also contribute to the overall advancement of AI in the financial sector.

## Author

**Aman Luther -** AFME AI Lead (amandeep.luther@afme.eu)