Illustrative Technical Considerations for Robust Post-Market Monitoring Evidence

Document ID: VSO-TECH-NOTE-PMM-001
Status: Non-Normative Technical Note
Date: December 2025
Prepared for: Technical consideration in PMM implementation discussions

---

Executive Summary

• Article 72 of the EU AI Act requires providers of high-risk AI systems to establish post-market monitoring (PMM) systems that actively and systematically collect performance data throughout system lifetime.

• The Regulation specifies PMM objectives but deliberately leaves implementation details open, creating practical questions around evidentiary robustness.

• PMM evidence may face scrutiny in post-incident investigations (Article 73) and supervisory reviews, where questions of data integrity and authenticity may arise.

• Mutable operational logs present inherent challenges for forensic reconstruction and may be subject to dispute regarding post-hoc modification.

• Tamper-evident logging mechanisms represent one possible technical approach that could strengthen the credibility of PMM evidence, though other valid approaches may exist.

• This note offers illustrative technical considerations only and does not advocate for any specific implementation methodology.

1. Regulatory Context

Article 72 of Regulation (EU) 2024/1689 establishes that providers of high-risk AI systems shall implement post-market monitoring systems in a manner proportionate to the nature of the AI technologies and their associated risks. Such systems must actively and systematically collect, document, and analyse relevant data throughout the AI system's lifetime.

The PMM obligation serves multiple regulatory functions: enabling continuous compliance evaluation against Articles 8–15 requirements, supporting the identification of emerging risks, and providing evidentiary foundations for corrective actions. Article 72(2) explicitly requires that PMM systems incorporate deployer feedback and real-world performance data, creating longitudinal evidence chains that may span years or decades of system operation.

Article 73 establishes parallel obligations for serious incident investigation, requiring providers to conduct investigations "without altering the AI system concerned in a way which may affect any subsequent evaluation of the causes of the incident." This preservation requirement implicitly extends to PMM data that may be relevant to incident reconstruction.

2. Practical PMM Implementation Challenges

The implementation of effective PMM systems raises several practical technical challenges that merit consideration:

Evidence integrity over time. PMM data must remain reliable throughout extended retention periods—potentially exceeding the 6-month minimum for logs (Article 19) and 10-year requirement for technical documentation (Article 18). Conventional data storage architectures may not inherently demonstrate that records have remained unaltered since their creation.

Traceability across system updates. High-risk AI systems typically undergo modifications during their operational lifetime. PMM systems must maintain coherent evidence chains that span multiple system versions, configuration changes, and model updates. Establishing which evidence applies to which system state introduces complexity in post-hoc analysis.

Post-incident reconstruction. When serious incidents occur, PMM data becomes forensic evidence. Investigators—whether internal, supervisory, or judicial—may question whether operational logs accurately reflect system behaviour at the time of the incident. The burden often falls on providers to demonstrate evidence authenticity.

Provider–deployer accountability boundaries. Article 26(6) establishes parallel log retention obligations for deployers. Where PMM systems depend on data from multiple parties, questions may arise regarding the provenance and integrity of data crossing organizational boundaries.

3. Illustrative Technical Considerations

One category of technical approaches that could address certain PMM evidence challenges involves tamper-evident logging mechanisms. Such mechanisms—well-established in domains including financial transaction systems, certificate transparency infrastructure, and digital forensics—employ cryptographic techniques to create verifiable records of data integrity.

At a conceptual level, tamper-evident logging may operate through several complementary mechanisms:

- **Sequential hash linking**, where each recorded event includes a cryptographic reference to its predecessor, creating chains where any modification would be computationally detectable.
- **Cryptographic timestamping**, which binds records to verifiable time references, addressing questions of temporal authenticity.
- **Aggregated commitment structures**, such as Merkle trees, which enable efficient verification of data subsets without requiring access to complete datasets.
- **Digital signatures**, which establish attribution and non-repudiation for human oversight actions.

Such mechanisms could, in principle, support PMM workflows by: providing mathematical evidence that logs have not been modified since creation; enabling third-party verification of evidence integrity without requiring trust in provider assertions alone; facilitating selective disclosure of relevant records while demonstrating dataset completeness; and creating audit trails that survive provider organisational changes or insolvency.

It should be emphasised that these represent illustrative possibilities. Other technical approaches— including trusted execution environments, third-party attestation services, or hybrid architectures—may offer comparable or complementary capabilities depending on specific implementation contexts.

4. Observations for PMM Workflows

Should tamper-evident approaches be considered for PMM implementation, several workflow integration points merit attention: evidence collection (PMM data sources could be captured within tamper-evident structures at the point of generation); supervisory access (market surveillance authorities could verify evidence integrity independently); incident response (pre-existing tamper-evident records could accelerate Article 73 investigations); and cross-party data flows (cryptographic provenance mechanisms could establish clear boundaries of responsibility).

These observations are offered as technical possibilities for consideration. The suitability of any particular approach would depend on factors including system risk classification, operational context, cost-benefit considerations, and alignment with forthcoming harmonised standards. It is expressly noted that minimum PMM compliance under Article 72 does not require any specific technical architecture.

Conclusion

This technical note has offered illustrative considerations regarding evidence integrity challenges in post-market monitoring under the EU AI Act. The observations are provided solely as one technical perspective for consideration by relevant stakeholders engaged in PMM implementation, harmonised standards development, or supervisory practice design. No specific approach is advocated, and it is acknowledged that multiple valid technical pathways may exist for achieving robust PMM evidence.

This document is non-normative and non-binding. It is provided for illustrative technical discussion only.