

Future proof your AI Investment

Ali Dootson, EQTY Life Sciences, Manchester, UK

ABSTRACT

As AI tools become integral to business functions, ensuring that they comply with the EU AI Act and embed model integrity throughout regulated workflows becomes essential. This paper explores how model cards—traditionally used as static documentation to clarify model construction and limitations—can be enhanced with cryptographic techniques, unified governance, and data and process lineage to support explainability and out-of-the-box compliance with the EU AI Act. By establishing traceability and control over AI systems, organizations can enable responsible AI practices and, importantly, measure model ROI alongside AI enablement efforts. As adoption advances, tackling both responsible AI and measurable impact becomes crucial for businesses to maximize their investments.

INTRODUCTION

As enterprises increasingly rely on machine learning models and AI-driven processes, the need for robust AI governance grows alongside. With AI embedded in regulated workflows, governance requires more than traditional IT principles, particularly as these systems demand substantial resource investments. According to Gartner, organizations that prioritize AI trust and transparency see a 50% improvement in adoption and acceptance, highlighting the need for governance frameworks that reinforce accountability and protect data integrity through cryptographic methods.

Currently, the value derived from AI is often gauged anecdotally, leaving early adopters unable to comprehensively measure the ROI of complex AI implementations. This paper examines how organizations and regulators can ensure trust by establishing verifiable oversight of model development, deployment, and maintenance practices to improve explainability and data quality across AI processes.

BUILDING A GOVERNANCE FRAMEWORK FOR AI

Unified Governance as a Foundation

A comprehensive governance framework is crucial to future-proofing AI investments, helping organizations manage ethical, legal, and operational responsibilities. Effective governance structures mitigate risks such as AI misuse, transparency gaps, and reputational damage while ensuring version control and compliance with evolving regulations.

Automated documentation, tracking, and auditing throughout the AI lifecycle—from data ingestion to model deployment—provide transparency and meet standards such as the EU AI Act, NIST, and Databricks and CIS security frameworks. In a recent IBM survey, 57% of IT professionals cited data privacy as the top barrier to AI adoption, followed by trust and transparency concerns (43%). Addressing these challenges requires a governance framework that ensures data provenance and integrity throughout its lifecycle, reflecting FDA guidance on the impacts of AI on data quality.

Privacy-focused regulations, such as the EU AI Act, mandate that individuals involved in real-world AI testing retain the right to withdraw consent and request data deletion. Cryptographic controls that prove anonymization and secure data access changes enable organizations to respect such privacy demands while maintaining AI system integrity.

DATA LINEAGE AND VERIFIABILITY

Data lineage—the ability to trace data origins, transformations, and flows within an AI system—forms a cornerstone of AI governance. Data quality risks, if unaddressed, can lead to biased models, unreliable outputs, and increased legal and compliance vulnerabilities. Menlo Ventures reports that 41% of executives find enterprise data challenging to integrate into AI, underscoring the need for automated attribution in model building and deployment.

By using cryptographic certificates, organizations create immutable records proving data integrity over time. This approach allows data and model integrity to be verified without exposing sensitive information, supporting both internal audits and external regulatory requirements. Cryptographic proofs also allow

third-party verifiability, creating a transparent AI system with trackable changes at every stage of data processing and transformation.

CRYPTOGRAPHY: THE FOUNDATION OF AI INTEGRITY

Why Integrity Matters

As AI models grow in complexity and use data from increasingly diverse and sensitive sources, governing these systems requires comprehensive tracking of each decision and data input. Cryptographic techniques such as verifiable compute and digital signatures offer a solution, enabling tamper-proof records that strengthen trust in AI.

According to Accenture, 90% of executives believe that multiparty systems, including cryptographic proofs, will be essential for building trustworthy AI. Cryptographic methods support compliance with the EU AI Act by enabling privacy-preserving measures such as pseudonymization, aligning with privacy-enhancing practices recommended by NIST and other standards.

VERIFIABLE AUDITS AND EXPLAINABILITY

As regulatory frameworks evolve, transparent and streamlined audits will be vital for ethical AI operations. Cryptographic proofs offer organizations a way to demonstrate compliance while maintaining data privacy and model confidentiality. For instance, zero-knowledge proofs allow organizations to confirm regulatory compliance without disclosing proprietary details. Such capabilities enhance explainability, especially in sectors like healthcare, where model transparency can directly impact patient outcomes.

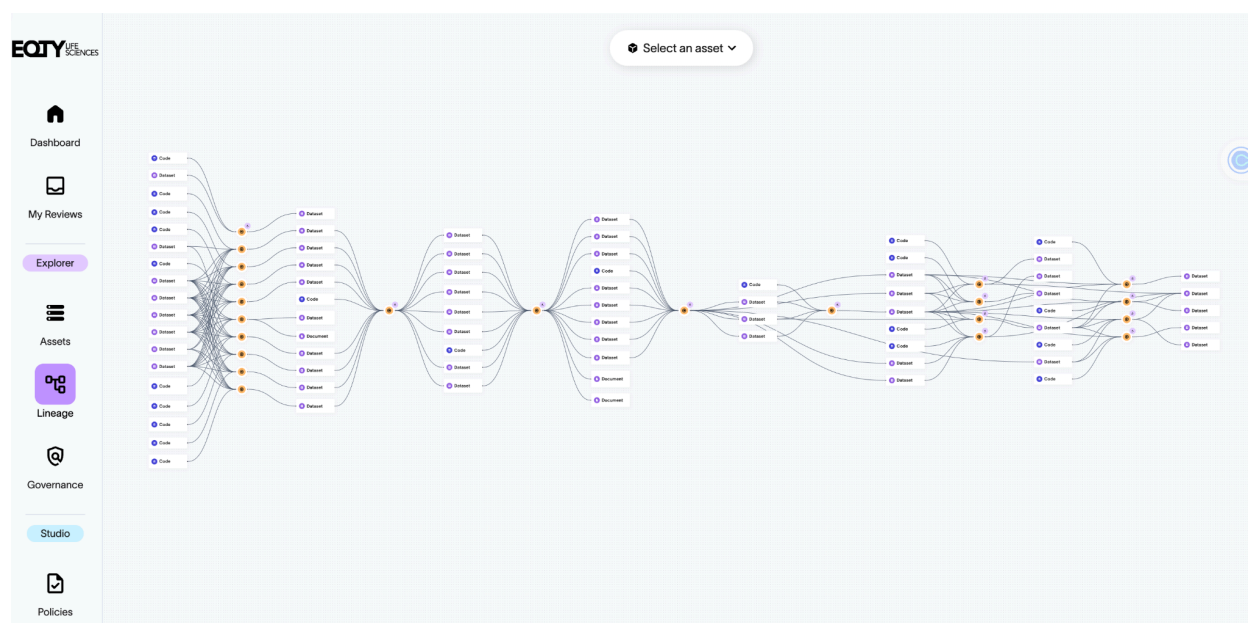
MODEL ATTRIBUTION AND ROI

In AI-driven workflows, establishing model attribution—linking the contributions of data sources, models, and other inputs—is essential for ROI assessment. As AI systems increasingly incorporate diverse data, models, and third-party services, attribution allows organizations to evaluate both the value and cost of these contributions effectively. Cryptographic certificates automate attribution and support compensation based on measurable value, aligning stakeholder incentives around data quality and reliability.

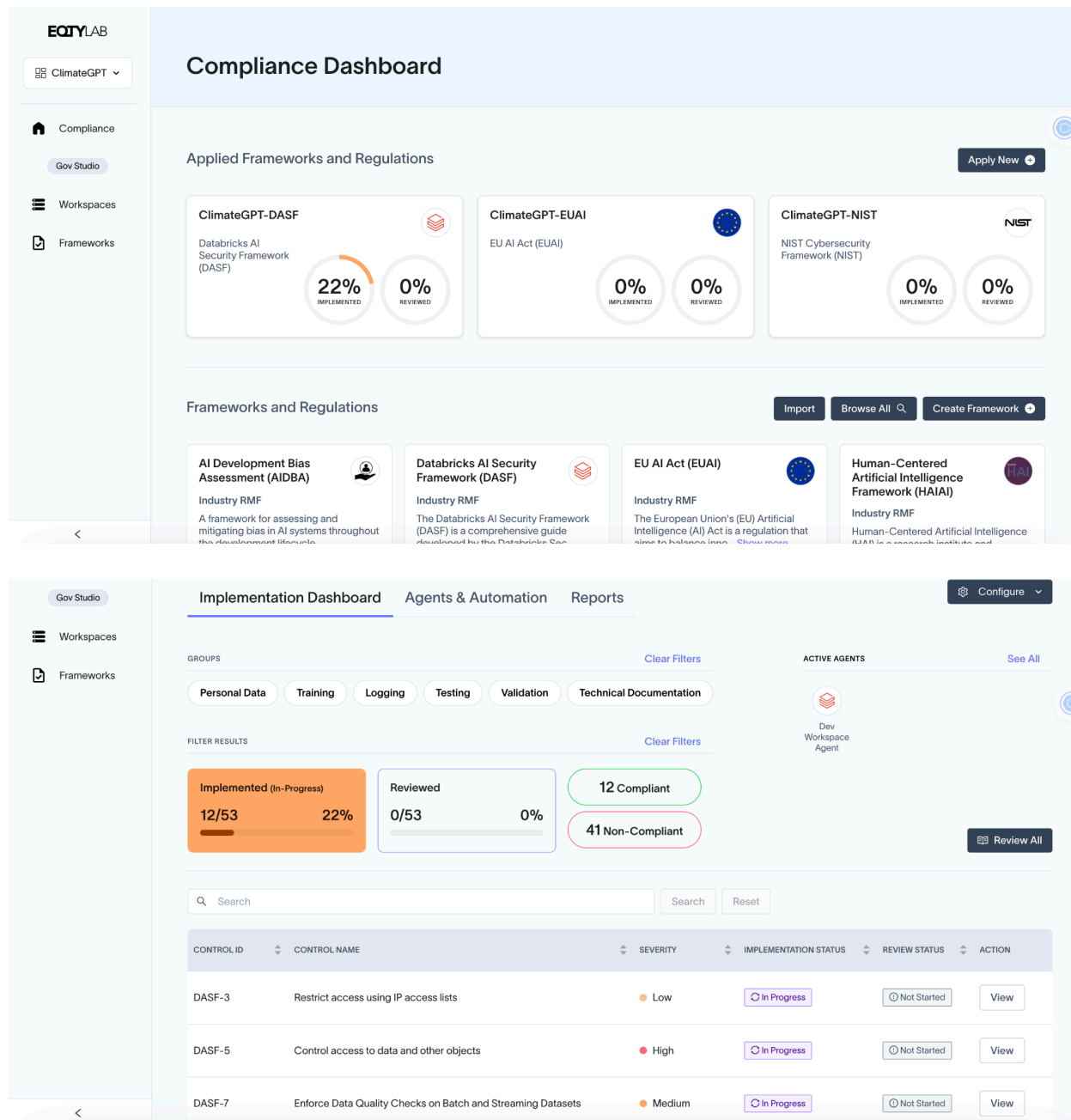
LINEAGE, GOVERNANCE, AND ATTRIBUTION: THREE PILLARS OF AI TRUST

These three pillars form the foundation of a trustworthy AI governance strategy:

- **Lineage:** Secure and verifiable data flow tracking ensures that data origins and transformations are documented, reinforcing compliance and data integrity.



- **Governance:** An automated governance framework ensures that AI processes comply with ethical and regulatory standards, using cryptographic integrity to create transparent, tamper-proof records.



- **Attribution:** Model attribution provides a mechanism for ROI evaluation, incentivizing data providers and model contributors based on the quality and impact of their contributions

PREPARING FOR THE AI OF TOMORROW

As AI regulations evolve, organizations must adopt flexible governance, lineage, and attribution solutions that adapt alongside AI advancements. Integrating cryptography into these frameworks ensures that organizations can maintain compliance and transparency as the regulatory landscape shifts.

CONCLUSION

In an AI-driven world, establishing transparent, compliant, and scalable governance frameworks is essential for safeguarding AI investments. By leveraging cryptographic techniques, organizations can create AI systems that meet regulatory requirements, uphold data privacy, and enable responsible innovation. As AI adoption continues, cryptography provides the trust and assurance needed to support transformative, compliant AI initiatives.

REFERENCES

<https://www.gartner.com/en/articles/what-it-takes-to-make-ai-safe-and-effective>
<https://newsroom.ibm.com/2024-01-10-Data-Suggests-Growth-in-Enterprise-Adoption-of-AI-is-Due-to-Widespread-Deployment-by-Early-Adopters>
<https://menlovc.com/2023-the-state-of-generative-ai-in-the-enterprise-report/>
<https://www.accenture.com/us-en/insights/blockchain/cloud-multiparty-systems>

ACKNOWLEDGMENTS

ChatGPT 4.0 assisted with some of the text

EQTY Research team put in countless hours researching text and developing materials used in the presentation

RECOMMENDED READING

https://www.ema.europa.eu/en/documents/scientific-guideline/reflection-paper-use-artificial-intelligence-ai-medicinal-product-lifecycle_en.pdf
<https://leg.colorado.gov/bills/sb24-205>
<https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence#next-steps-7>

CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the author at:

Author Name: Ali Dootson

Company: EQTY Life Sciences

Email: alistair.dootson@eqtylab.io

Website: eqtylab.io

Brand and product names are trademarks of their respective companies.