

Regulatory One-Page Summary

United States

Regulatory Context

US financial regulators emphasize data integrity, auditability, third-party risk management, operational resilience, and model risk governance. Supervisory expectations are principles-based and enforced through examination, rather than prescriptive technical mandates.

Regulatory Problem Addressed

Sensitive data is often distributed across applications, vendors, and environments, creating gaps in integrity, access traceability, and audit evidence. These gaps increase supervisory, operational, and litigation risk.

EpositBox Control Approach

EpositBox operates as an independent data custody platform that enforces immutable data integrity, zero-trust access, and provable audit trails.

Key control characteristics include:

- Immutable, blockchain-anchored records
- Machine-to-machine access with deterministic authentication
- Full access history and data lineage
- Separation of data custody from application logic

AI Risk Alignment

EpositBox does not perform AI decision making. It provides high-integrity data foundations that support explainable and reviewable AI usage, aligning with SR 11-7 model risk expectations and supervisory guidance on AI governance.

Operational Resilience

Immutable records and deterministic recovery support incident response, forensic review, and supervisory reporting without reliance on log reconstruction.

Supervisory Takeaway

EpositBox reduces systemic data risk by improving integrity, auditability, and accountability across the data lifecycle, supporting US regulatory objectives for safety, soundness, and transparency.