

**v3.4-OPS-003 – Operational Metrics, Runtime Observability & Policy
Replay Audit**

Document Title	Operational Metrics, Runtime Observability & Policy Replay Audit
Version	v3.4
Document ID	v3.4-OPS-003
Date	2025-03-22
Author	Take Back Your Data – Autonomous Operations Unit
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines operational observability, metrics architecture, and policy replay auditability for MaxOneOpen forks. It ensures that all runtime behavior is traceable, predictable, and certification-compliant.

2. Metrics & Observability Stack

- All forks must expose runtime metrics via sealed observability endpoints
- Metrics must be schema-bound and runtime-agnostic
- Key indicators include: uptime, twin event frequency, resource drift, latency anomalies
- Observability stacks must be fork-local and cryptographically verifiable

3. Policy Replay & Audit Tracing

Replay Element	Purpose	Validation Hook
Twin State	Baseline vs. anomaly map	Snapshot hash + schema link
Execution Path	Trigger causality replay	Sealed trace anchors
Policy Stack	Governance override trace	ZK-policy audit log
Audit Trail	End-to-end policy impact	Delta fingerprint match

4. Certification Hooks

- All runtime behavior must be reconstructible from sealed metrics and audit anchors
- Metrics APIs must be namespace-bound and non-extractable
- Policy replay must prove full lifecycle traceability

5. Certification Triggers

- Opaque metrics stacks or audit gaps disqualify forks
- Runtime events without traceable trigger policy invalidate certification

6. Certification Relevance

Certified MaxOneOpen forks must implement observability and audit mechanisms enabling verifiable runtime behavior. Operational trust is only possible through replayable policy paths and sealed execution logic.