

v3.4-SCN-002 – Schema-Aware Policy Testing & Runtime Compliance Hooks

Document Title	Schema-Aware Policy Testing & Runtime Compliance Hooks
Version	v3.4
Document ID	v3.4-SCN-002
Date	2025-03-22
Author	Take Back Your Data – Compliance Architecture Group
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines schema-aware policy testing mechanisms and runtime compliance hook architecture in MaxOneOpen. It ensures automated evaluation of declared policies and provable runtime enforcement logic for certified forks.

2. Policy Test Harness

- Forks must expose all declared schema policies via test harness
- Tests must simulate misuse, drift, overload and override
- Each policy failure must produce a runtime alert or hard-stop
- Harness logic must be ZK-auditable and schema-linked

3. Runtime Compliance Hook Architecture

Hook Type	Trigger Condition	Response Mechanism
Pre-Exec Hook	Policy mismatch	Abort + ZK log
Live Guard Hook	State drift	Alert + isolate
Post-Result Hook	Schema violation	Rollback + traceproof
Control Override Hook	Manual flag	Audit flag + twin notify

4. Certification Interface Logic

- Compliance hooks must be observable via certification test run
- Forks must prove coverage of declared enforcement domains
- Hooks must include outcome proof and policy traceability
- Overrides must be logged with verifiable author stamp

5. Certification Triggers

- Gaps in hook coverage or test mismatch revoke certification
- Dynamic policy updates must trigger full revalidation
- Missing audit visibility into override events disqualifies fork

6. Certification Relevance

Schema-aware policy testing and runtime compliance hooks are required for MaxOneOpen certification. Certified forks must offer full traceable and testable enforcement visibility.