

v3.4-DAT-002 – Data Governance, Provenance & Schema Validation

Document Title	Data Governance, Provenance & Schema Validation
Version	v3.4
Document ID	v3.4-DAT-002
Date	2025-03-22
Author	Take Back Your Data – Data Provenance Unit
Document Type	Public / Certification / Internal

1. Purpose & Scope

This document defines the data governance framework, provenance validation logic and schema enforcement mechanisms used within MaxOneOpen. It ensures that all data origins are traceable, policies enforceable and schema behavior predictable across deployments.

2. Governance Policy Model

- Governance policies are defined per schema domain
- User-driven overrides must be cryptographically signed
- Governance includes encryption, access, retention and usage rights
- Forks must implement dynamic governance triggers and logs

3. Provenance Tracking Logic

Element	Source Record	Validation Mode
Data Entry	Signed creation metadata	Hash proof + timestamp
Transformation	Twin ID + hash delta	Reversible state chain
Schema Enforcement	Schema ID + rule log	Local contract enforcement
Export Event	External target signature	Destination log & commit hash

4. Schema Validation Logic

- Each data object must match an active schema definition
- Validation includes type, format, constraint and role scope
- Runtime schema mismatch results in data rejection or quarantine
- Forks may define custom schema dialects if declared + mapped

5. Runtime Enforcement & Audit

- All schema and provenance actions must be audit-logged
- Local runtime must enforce rules without cloud resolution
- Forks must expose policy triggers and allow external verification
- Certification requires full data lineage reproducibility

6. Certification Relevance

Schema enforcement and data governance are core MaxOneOpen certification requirements. Deployments must trace, validate, and enforce all schema-bound data activities cryptographically and independently.