

## **MaxAudit – MaxControl Integration & Twin Interaction**

Version: 1.0

Issued by: SAC, Take Back Your Data (TBYD)

License: MaxOneOpen License v2.2 – Structurally Enforced

### **1. Context & Purpose**

This module describes how MaxAudit integrates with MaxControl and the MaxInstance Twin system to enable real-time, architecture-aligned auditing. MaxControl orchestrates the activation and suspension of MaxInstances, including their Twins, based on current system conditions and audit feedback.

### **2. Role of MaxControl**

- Coordinates system state across Machinespace
- Activates Twins based on workload, topology, or risk profile
- Relays structural configuration to MaxAudit for live validation
- Reacts to audit signals (e.g. yellow/red) by isolating affected modules

### **3. Audit-Aware Twin Management**

MaxAudit receives dynamic state metadata from MaxControl, including:

- Active/Inactive Twin Map
- ZKP anchoring status of each Twin
- Hash-based instance integrity proofs
- Submodule activation logic

This enables:

- Auditing only of active components
- Real-time adjustment of audit scope
- Detection of unauthorized activation paths

### **4. Secure Signaling Interface**

- One-way signal channel from MaxAudit to MaxControl
- Signals are cryptographically signed status tokens
- MaxControl uses these to enforce isolation, rescheduling, or module blocking

### **5. Use Cases**

- Isolation of a non-compliant Twin after failed self-test
- Temporary suspension of modules pending yellow remediation

- Prevention of fork mismatches during live updates
- Enforcement of audit pause during cryptographic inconsistency

## **6. Determinism & Verification**

MaxControl maintains an auditable state ledger of all Twin changes, ensuring:

- Verifiable sequence of all structural events
- Tamper-proof activation history
- Cross-validation with MaxAudit results in output protocol