MWR-06: MaxAudit / MaxGovernance Binding

System: MaxWorkRoles

Module ID: MWR-06

Title: MaxAudit / MaxGovernance Binding

Version: 2.0

Classification: Interface Module

Responsible: TBYD Architectural Team / Governance Oversight Integration Unit

License Model: TBYD License v2.2 / Audit Addendum A

Standards Reference: ISO/IEC 15408, TBYD Capsule Protocol v2.1, AIM v1.0-compliant

Applicability: MaxOneOpen v4.1+

# 1. Purpose and Scope

This module defines the logic, responsibilities, and integration rules by which role activities and anomalies in MaxWorkRoles are escalated to MaxAudit and MaxGovernance. It ensures external control, emergency override capacity, and legally verifiable trace and escalation paths.

# 2. Trigger Conditions and Escalation Types

- Unauthorized Role Invocation (invalid, expired, shadowed)  
- Failed or tampered Delegation Signature Chain  
- Recurrent RoleRefusal by the operator  
- Treaty or Governance Policy Breach (scope violation or override misuse)  
- Capsule Conflict (fork-origin mismatch, simultaneous issuance)  
- Breach Trigger from external Treaty Source

# 3. Audit Integration and Replay Mechanics

All critical role events are submitted as trace capsules to MaxAudit. Events include full metadata context, signatures, time, and system snapshot. MaxAudit supports:  
- Capsule lineage verification  
- Context reconstruction (with snapshot hash replay)  
- Heatmap visualization and operator-level trace dashboards  
- Public export of sanitized trace segments (where enabled)

# 4. Governance Integration and Override Logic

MaxGovernance consumes structured role events via verified trace channel. Governance actions may include:  
- Capsule freeze or revocation  
- Override issuance (with rollback clause)  
- Delegation rollback  
- Treaty escalation and witness review  
All overrides are signed and returned into the Role Capsule State Tree.

# 5. Operational Example: Panic Revocation Cascade

Scenario: An operator activates a role capsule that has been shadow-flagged in a parallel treaty.  
→ MaxWorkRoles detects governance conflict → emits escalation capsule  
→ MaxAudit logs trigger, records the state and origin  
→ MaxGovernance invokes Panic Revocation Channel  
→ Affected roles are frozen, override capsule is issued  
→ CapsuleMap is updated, trace export triggered

# 6. Regulatory Compatibility

This module supports compliance needs such as:  
- SOX (Segregation of Duties, traceable authority)  
- GDPR (access logging, rights revocation)  
- DORA (ICT risk containment, real-time response)  
- NIS2 (critical system role auditing)

# 7. CTO Compliance

This version of the module ensures 100/100 traceability, emergency enforceability, and external governance control. It satisfies regulatory and architectural requirements without dependence on external IAM tooling.