# Module XX – IAM & Role Enforcement Layer (Capsule-Based Runtime Access Control)

Version: 4.1 | Classification: CTO Mandatory (Governance Enforcement)

Scope: Role definition, trust-tier mapping, runtime control capsule logic

## 0. Purpose & Operational Governance

This module defines the capsule-anchored identity and access control layer for MaxOneOpen v4.1. It translates organizational roles into enforceable runtime permissions via capsule boundaries, trust tier declarations, and signature-bound access validation. It enables operational enforcement, policy compliance, and federation-safe runtime control without relying on external IAM tools.

## 1. Identity Types & Trust Role Mapping

Defined identities:  
- Sovereign Root (Tier 0)  
- Capsule Signer (Tier 1)  
- Audit Validator (Tier 2)  
- Rule Injector / Policy Agent (Tier 3)  
- Operational Observer / Add-on Validator (Tier 4)  
- Sandbox Entity (Tier 5)  
Each identity must bind a unique signing key, ledger ID, federation scope and declared role tier in its `Role Declaration Capsule (RDC)`.

## 2. Role Declaration Capsule Format

Each runtime actor must emit a `Role Declaration Capsule (RDC)`:  
`{ rdc\_id, entity\_id, role\_class, trust\_tier, federation\_zone, signature, expiration, policy\_scope[] }`  
- Signature must be verifiable back to Tier 0 or 1  
- Expired or untraceable RDCs are invalid for capsule execution

## 3. Enforcement Logic at Runtime

Runtime enforcement engine must:  
- Check each capsule’s emitter against current RDC registry  
- Enforce tier boundary (no capsule execution above declared tier)  
- Trigger `Trust Violation Capsule (TVC)` on mismatch  
- Apply suspension if `policy\_scope` is exceeded (e.g. fork attempt by Tier 3)

## 4. Federation Role Inheritance & Cross-Zone Trust

- Cross-zone actors must be listed in the FCC (Federation Consent Capsule)  
- Their RDCs must specify `federation\_zone` and be co-signed by the receiving zone Tier 1  
- Federation divergence without co-confirmed RDC invalidates execution rights

## 5. IAM Ledger Overlay & Audit Access Map

- All RDCs must be ledger-committed and visible via `/iam/overlay/{role\_class}`  
- Each ledger entry includes policy hash, role class, TTL and active zone  
- Observer and Audit roles may inspect IAM overlays without execution privilege