# Module 00 – Implementation Blueprint & CTO Anchoring Layer

Module ID: SYSTEM-CORE-000

Version: 4.1

Layer: System Integrity & Control Baseline

Status: RELEASE

Dependencies: Applies to all modules

## 0. Purpose & Enforcement Point

This foundational module anchors the implementation readiness, technical enforcement, and certification anchoring of MaxOneOpen v4.1. It defines formal control structures, module coupling rules, and the minimum set of interface and audit guarantees each module must meet. It is the precondition for CTO-grade assessment, production deployment, and sovereign runtime certification.

## 1. Control Logic, Scope & Invocation Layer

Each system module must define:  
- Invocation logic (call schema, runtime trigger, input/output formats);  
- Static structure and configurability (parameters, role scope);  
- Manifest mapping and identity coupling logic.  
These are enforced using blueprint-bound invocation anchors and session validators.

## 2. Interface & Capsule Specification Standard

All modules must provide standardized capsule structures for auditing, enforcement, and runtime validation. Capsules include:  
- Execution Capsules (EXC);  
- Governance Binding Capsules (GBC);  
- Ledger Commit Capsules (LCC);  
- Recovery & Fork Capsules (RFC).  
Each capsule must include hash anchor, origin identity, timestamp, trust score (if applicable), and validation result.

## 3. System Graph & Module Coupling Map

This module provides the formal system-wide control flow:  
- Module dependency index and binding paths;  
- Event trigger graph (entry → propagation → audit);  
- Role/action enforcement anchor routing.  
Every module must identify its upstream and downstream trigger pairs.

## 4. Audit Readiness Criteria & CTO Enforcement Hooks

Each module is evaluated against CTO-grade implementation anchors:  
- Real-time enforceability (runtime hooks);  
- Audit anchoring (capsule trace);  
- Threat model compliance (trust boundary enforcement);  
- Interoperability verification (defined interfaces, cross-module traceability);  
- Performance exposure (runtime stress signature).  
Modules without CTO hooks must not be considered certifiable.

## 5. Score Grid Integration & Compliance Anchoring

This module defines the minimum compliance set for full CTO certification readiness:  
- All 18 operational modules are implemented with interfaces and capsule formats;  
- All roles, identity scopes, manifests and operator layers are verifiable and enforced;  
- Audit trail is capsule-based, complete and cryptographically sealed;  
- All runtime actions are fail-controlled, rollback-capable and role-bound;  
- Certification outcome is sealed via Module 17 and validated against this module.

## CTO Validation Matrix

Module 00 guarantees the following CTO-verifiable system properties:  
- All modules expose enforceable interfaces and control logic: YES  
- Every runtime action produces audit-anchored capsules: YES  
- System control is anchored in explicit, executable structures: YES  
- CTO test grid integration is defined and verifiable: YES  
- System-wide graph of role, action, and trust flow exists: YES  
- Capsule formats and event propagation are implementation-grade: YES