

### v3.4-FINAL-005 – Twin Compliance Checklist & Approval Workflow

This document defines the twin-level compliance checklist and approval workflow for all runtime components and modules within certified MaxOneOpen v3.4 forks. All listed conditions must be met and cryptographically notarized before deployment.

Component / Module	Compliance Criteria	Verification Method	Approval Required?
Runtime Container	Version pin matches certified digest	SHA-256 hash match	✓ Yes
Twin Capsule	Schema-bound + sealed signature	ZK Capsule Proof	✓ Yes
Execution Policy	No unscoped IO or memory access	Policy Trace Replay	✓ Yes
Communication Relay	Channel-sealed, zero-state	Relay Certificate + Twin Signature	✓ Yes
Fork Root Key	Matches registered issuer + is valid	Signature Path + Expiry	✓ Yes
Edge Node	Signed boot + verified anchor	Device Trust Proof	✓ Yes
Model Fork	Schema-isolated, audit-ready	Fork Capsule Digest	✓ Yes
Data Access	Consent-driven + revocable	Consent Token + Access Trail	✓ Yes
ZK Query Layer	No plaintext access to index	ZK Proof Chain	✓ Yes
P2P Twin Sync	Dual signature with conflict win proof	Signature Resolution Log	✓ Yes
Vault Container	Sealed local store, schema-bound	Storage Digest + Proof	✓ Yes
Lifecycle Logic	All states terminable + traceable	Status Log with TTL	✓ Yes