MaxDeploy v1.0 – CTO Verification Checklist

This document provides a CTO-focused checklist to verify the validity, trustworthiness, and governance compliance of any deployment executed via MaxDeploy. It enables structured inspection of technical, legal, and operational readiness.

# 1. Deployment Legitimacy

* ✅ Was the deployment capsule signed by an authorized operator?
* ✅ Does the operator role match the assigned execution scope?
* ✅ Is the deployment intent manifest verifiable and complete?

# 2. Policy Compliance

* ✅ Was a valid `policy.ref` included and matched in MaxReg?
* ✅ Were all preconditions and regulatory assertions fulfilled?
* ✅ Did the system correctly block policy-violating intents?

# 3. Auditability and Export

* ✅ Is there a `meta.audit.json` file signed and timestamped?
* ✅ Does `audit.trace.sig` contain the full integrity hash path?
* ✅ Can the deployment be externally verified in an air-gapped environment?

# 4. Governance and Licensing

* ✅ Was the license class validated against the license registry?
* ✅ Does the deployment reference a legally signed `anchor.ref`?
* ✅ Has the deployment been checked for unauthorized fork attempts?

# 5. Technical Reproducibility

* ✅ Is the deployment capsule reproducible on compliant MaxOneOpen nodes?
* ✅ Are the manifest and all upstream anchors hash-locked?
* ✅ Can the full deployment state be regenerated using the xID?

# 6. Responsible Signature Chain

* ✅ Is the deployment signed by a verifiable individual or org unit?
* ✅ Does the signature chain include operator and policy notary?
* ✅ Is the revocation status of all related keys valid?