# MaxSuite – System Role and Boundary

Version: 1.0

Module ID: 00

Document Type: Subsystem Definition

---

## 1. Systemic Role of MaxSuite

MaxSuite provides a containerized execution environment for open-source applications (such as LibreOffice, Jitsi, or similar) within a governed and auditable runtime. It does not deliver the applications themselves, but encapsulates, signs, and enforces their policy-based execution using capsule logic. MaxSuite acts as a governance-anchored gateway between system integrity and end-user application access.

## 2. Boundary Definition

MaxSuite does not replace full desktop environments or generic container stacks (like Docker or Flatpak). Instead, it operates as a runtime-level app container for policy-bound application use inside MaxOneOpen infrastructures.  
  
It enforces the following boundaries:  
- No runtime escalation beyond defined roles  
- No uncontrolled network access without policy  
- No file system exposure outside of signed capsule paths  
- All execution must be auditable and rollback-capable

## 3. Integration into the MaxOneOpen Stack

MaxSuite is tightly integrated with:  
- MaxReg (policy anchoring per application capsule)  
- MaxDeploy (capsule distribution and execution control)  
- MaxAudit (audit hook for runtime execution)  
- MaxGovernance (role-based execution authorization)

## 4. Optional Federation Context

In cross-organization environments, MaxSuite capsules may be referenced and validated by federation-level agreements. For this purpose, MaxTreaty can be used to issue runtime-wide app execution constraints or override pathways.