

Tier-1 Defensibility Map – Physical + Cyber Overlay

Where physical access invalidates cyber assumptions (audit, investigation, litigation view)

Governance Layer	Cyber Assumption	Physical Reality	Defensible Control / Evidence
Identity & Authentication	Device trust, MFA, keys protected No insider access assumed	Console, port, badge, or rack access Enables credential capture or bypass	Restricted physical access Badge logs + CCTV + tamper alerts Key storage controls
Cryptography & Keys	Keys stored in HSM / enclave Crypto boundaries enforced	Physical access enables probing, firmware extraction, cold boot	HSM tamper evidence Key rotation evidence Physical inspection records
Logging & Forensics	Logs complete and trustworthy	Local log deletion or alteration before aggregation	Centralized immutable logging Physical access correlation
AI & Control Systems	Model integrity and data pipeline trusted	Sensor spoofing or model tampering via physical access	Model validation + fallback Physical sensor protection
Incident Response	Cyber-only containment sufficient	Evidence loss without physical control Chain-of-custody risk	Joint cyber + physical IR Access freeze + evidence control

Why This Overlay Matters

For Tier-1 systems, physical access collapses many cyber-only assumptions. This overlay demonstrates that governance explicitly accounts for that collapse, ties physical controls to cyber risk treatment, and preserves evidentiary integrity. This is a critical factor in regulatory reasonableness assessments and post-incident scrutiny.