

Enterprise Technology Risk Governance – Defensibility Map

Regulator-Facing Alignment (NIST • ISO • EU)

1. Governing Authority	2. Scope Control	3. Exposure Identification	4. Assumption Control
Enterprise risk framing • OECD Digital Security Risk Mgmt • NIST SP 800-30 • ISO/IEC 27005	Tier-1 system designation • NIST SP 800-53 (PL, RA) • ISO/IEC 27001:2022	Pre-auth, crypto, AI, physical exposure • NIST SP 800-53 (IA, SI, SR) • MITRE ATT&CK; • ENISA PQC guidance	Documented assumptions w/ expiry • ISO/IEC 27005 • NIST SP 800-30
5. Decision Traceability	6. Stress Testing	7. Review & Adaptation	8. Defensible Position
Mitigate / Accept / Deprecate • ISO/IEC 27001 risk treatment • NIST SP 800-53 (PM, PL)	Realistic exploitation scenarios • NIST SP 800-61 / 800-184 • MITRE ATT&CK-based; testing	Scheduled executive review • ISO/IEC 27001 continual improvement • NIST governance lifecycle	Reasonable foresight standard met • EU AI Act (risk-tiered governance) • OECD accountability principle

Regulatory Defensibility Summary

This governance model aligns with internationally recognized standards (NIST, ISO, OECD, EU) and demonstrates reasonable, good-faith risk management rather than claims of absolute security. Explicit scope definition, documented assumptions, executive decision records, and repeatable review cadence address the core questions regulators ask: what was known, who decided, and how governance adapted.

Audit / Investigation Readiness

Artifacts are evidence-first and producible on demand: Tier-1 registers, assumption logs, risk treatment decisions, stress-test outputs, and review records. This structure resists hindsight bias and supports proportional enforcement analysis.