

# 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 <ul style="list-style-type: none"><li>• OECD Digital Security Risk Mgmt</li><li>• NIST SP 800-30</li><li>• ISO/IEC 27005</li></ul>	Tier-1 system designation <ul style="list-style-type: none"><li>• NIST SP 800-53 (PL, RA)</li><li>• ISO/IEC 27001:2022</li></ul>	Pre-auth, crypto, AI, physical exposure <ul style="list-style-type: none"><li>• NIST SP 800-53 (IA, SI, SR)</li><li>• MITRE ATT&amp;CK;</li><li>• ENISA PQC guidance</li></ul>	Documented assumptions w/ expiry <ul style="list-style-type: none"><li>• ISO/IEC 27005</li><li>• NIST SP 800-30</li></ul>
5. Decision Traceability	6. Stress Testing	7. Review & Adaptation	8. Defensible Position
Mitigate / Accept / Deprecate <ul style="list-style-type: none"><li>• ISO/IEC 27001 risk treatment</li><li>• NIST SP 800-53 (PM, PL)</li></ul>	Realistic exploitation scenarios <ul style="list-style-type: none"><li>• NIST SP 800-61 / 800-184</li><li>• MITRE ATT&amp;CK-based; testing</li></ul>	Scheduled executive review <ul style="list-style-type: none"><li>• ISO/IEC 27001 continual improvement</li><li>• NIST governance lifecycle</li></ul>	Reasonable foresight standard met <ul style="list-style-type: none"><li>• EU AI Act (risk-tiered governance)</li><li>• OECD accountability principle</li></ul>

## ***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.