

Regulator-Facing Governance Narrative

What We Knew, When We Knew It, and Why We Decided

Governance Standard

The organization applies a reasonable foresight and good-faith governance standard aligned with NIST, ISO/IEC, OECD, and EU risk-tiered governance principles. Absolute security is not asserted; decision traceability, assumption control, and evidence preservation are the governing objectives.

What Was Known

Tier-1 systems were explicitly designated. Internet and identity-adjacent exposures were continuously inventoried with executive ownership, remediation clocks, and isolation capability. Load-bearing assumptions were explicit, owned, and time-bound.

When It Was Known

Exposure awareness was continuous. Assumptions were reviewed on cadence and upon credible contradictory evidence. Executive decisions were recorded contemporaneously with available information and explicit expiration dates.

Why Decisions Were Taken

Decisions prioritized impact, exposure duration, and assumption dependency. Executives were authorized to immediately reduce exposure or degrade service when assumptions collapsed or remediation timelines exceeded approved bounds. Delay pending certainty was prohibited.

Evidence Preservation

Tier-1 evidence sources were centrally logged, time-synchronized, retained for ≥ 180 days, and subject to predefined legal-hold triggers. Failure to preserve or produce evidence within 24 hours constitutes a governance failure.

Review and Adaptation

Post-event review invalidates fragile assumptions, updates stress scenarios, and evaluates executive decision behavior to ensure governance adapts to observed reality.

Defensibility Statement

At all times the organization can demonstrate what was known, who decided, when decisions were made, why they were reasonable, and how evidence was preserved, supporting proportional regulatory assessment and resisting hindsight bias.

Role	Name	Signature	Date
CEO			
CISO			
CIO			
General Counsel			
Board Risk / Audit Chair			