TR-001: Standards Alignment & Regulatory Compliance

Date: January 25, 2026

Author: Kalyb Prince

Status: Sovereign Release for Industrial Certification

1. Overview of Alignment Strategy

The TR-001 framework is engineered to satisfy the "rigorous deterministic governance" mandates established during the **2026 Davos Convergence**. It provides a repeatable "operating system" for compliance, using mathematical axioms to fulfill the legal requirements of the EU AI Act and the management controls of ISO/IEC 42001.

2. ISO/IEC 42001: AI Management System (AIMS) Mapping

TR-001 axioms provide the technical "how" for several certifiable Annex A controls:

- **Control A.6 (AI System Life Cycle):** The **1.12 Reasoning Floor** acts as a mandatory "Quality Gate" for every recursive step, ensuring that model performance never drops into unmanaged probabilistic drift.
- **Control A.7 (Data for AI Systems):** The **12-Link Limit** provides the "Data Provenance" required for auditable records. It enforces a forensic boundary where information lineage is mathematically guaranteed before entropy takes over.
- **Control A.10 (Monitoring & Measurement):** The **1.81 Stability Constant (S_c)** serves as a deterministic Key Performance Indicator (KPI). Unlike legacy systems that rely on vague drift detection, TR-001 uses S_c to monitor system health in real-time.

3. EU AI Act: High-Risk AI Obligations

TR-001 is positioned to meet the 2026 enforcement deadlines for high-risk and General Purpose AI (GPAI) systems:

- **Article 17 (Quality Management System):** The **Technical Specification (TR001-SPEC-STABILITY-2026)** provides the "systematic and orderly documentation" required for conformity assessments.
- **Article 50 (Transparency & Labeling):** The framework ensures that all AI-generated outputs are identifiable in a "machine-readable format." By identifying **1.809** as a

non-recoverable error state, TR-001 enables automated isolation of "hallucinatory" content before it reaches the end-user.

- **Technical Robustness (Article 15):** The **1.81 Equilibrium** fulfills the requirement for resilience against adversarial attacks. Any attempt to manipulate the substrate is detected as a deviation from the S_c baseline, triggering a 1.12 Hard Floor reset.

4. Forensic Traceability & Audit Trails

TR-001 satisfies the 2026 "Operational Evidence" standards by providing:

- **Immutable Audit Trails:** Every reasoning step up to the **12-Link Limit** is a signed event, allowing for the temporal reconstruction of decisions required by financial and critical infrastructure regulators.
- **Signed Logs:** By designating 1.809 as a failure threshold, the framework generates "Negative Evidence" (logs of what the system *rejected*), which is now a critical component of regulatory audits.

TR-001 Compliance Matrix: Axiom-to-Standard Mapping

TR-001 Axiom / Control	ISO/IEC 42001 Control (AIMS)	EU AI Act Article	Compliance Function & Regulatory Evidence
1.12 Reasoning Floor	**Control A.8.2:** AI System Lifecycle Management	**Article 17:** Quality Management System	Functions as a mandatory "Quality Gate" ensuring reasoning links never drop into unmanaged probabilistic drift.
1.81 Stability Constant (S_c)	**Control A.10.2:** Monitoring and Measurement	**Article 15:** Accuracy, Robustness, & Cybersecurity	Provides a deterministic KPI for monitoring system health and "Substrate Stillness" in real-time.
1.809 Failure Threshold	**Control A.8.4:** AI System Impact Assessment	**Article 15(4):** Fail-safe Plans and Resilience	Automates system isolation and reset protocols, acting as a technical fail-safe against "Decay Cascades".
12-Link Limit	**Control A.7:** Data Governance & Traceability	**Article 50:** Transparency & Provenance	Establishes a forensic boundary where information lineage is mathematically guaranteed, fulfilling Article 50's disclosure mandates.
ANEV Methodology	**Control A.8.2:** Design Verification	**Article 17(1)(b):** Design and Development Procedures	Supplies the "Techniques and Systematic Actions" required for the documented design control of high-risk AI systems.