AI Governance for Agentic RevOps

NIST • EU AI Act • ISO 42001



Turning Compliance into Competitive Velocity.

John Utley, Founder & Fractional Agentic AI Advisor | Sophizo.net

The Braking Paradox of B2B SaaS

Adoption

88% of organizations use AI,
72% use Gen AI
(McKinsey State of AI 2025).

Scaling

23% of organizations are actively scaling agentic AI.



The Mandate

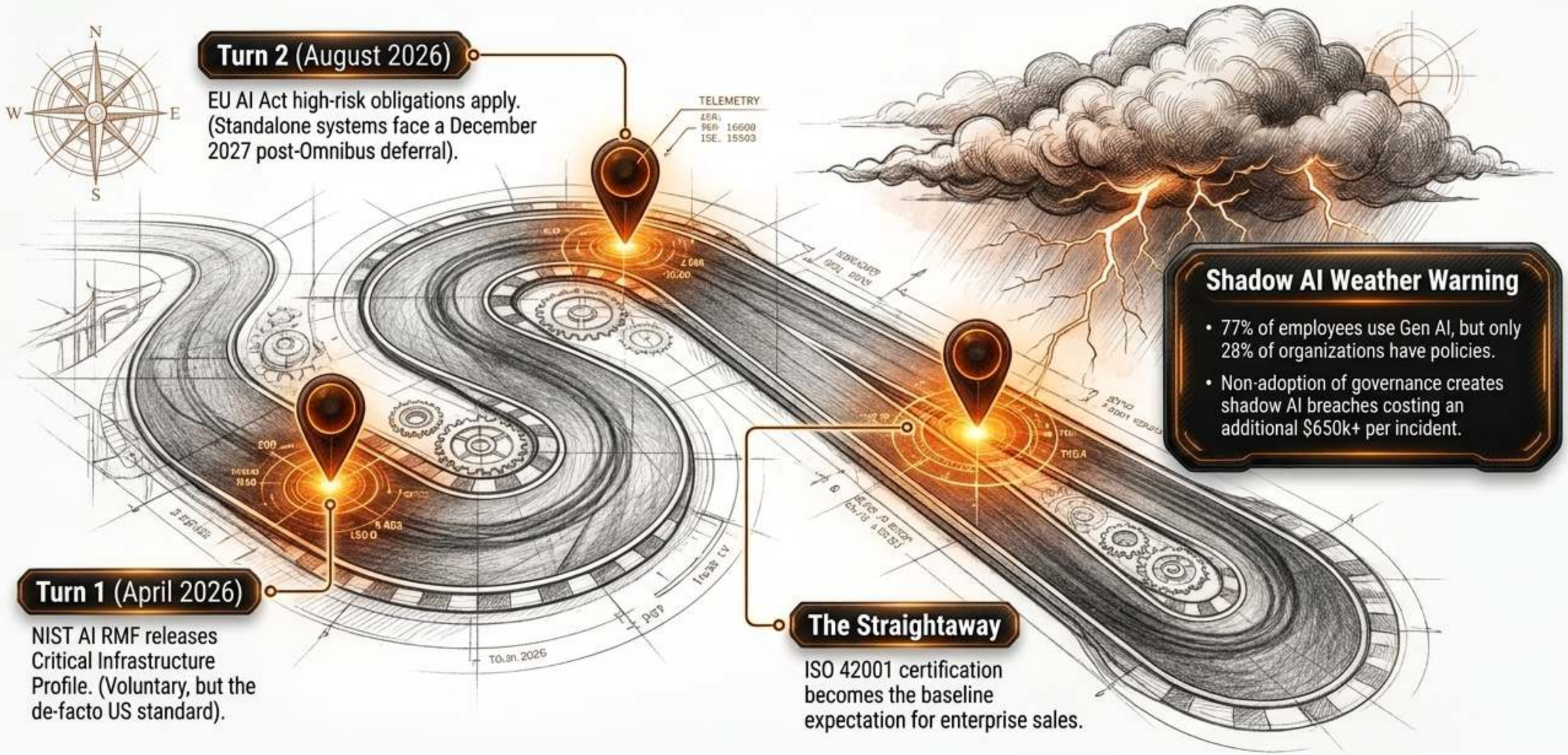
Boards now demand provable controls before approving Go-To-Market (GTM) motions.

The Threat

$4.4B in AI-related losses industry-wide in 2025 alone.

The Paradox: Sophisticated brakes aren't designed to stop a race car: they are engineered so the driver can corner faster. Ignoring governance is not agility, it is negligence that directly threatens ARR, valuation, and exit multiples.

Upcoming Track Conditions and Regulatory Hazards



Turn 2 (August 2026)

EU AI Act high-risk obligations apply. (Standalone systems face a December 2027 post-Omnibus deferral).

Turn 1 (April 2026)

NIST AI RMF releases Critical Infrastructure Profile. (Voluntary, but the de-facto US standard).

The Straightaway

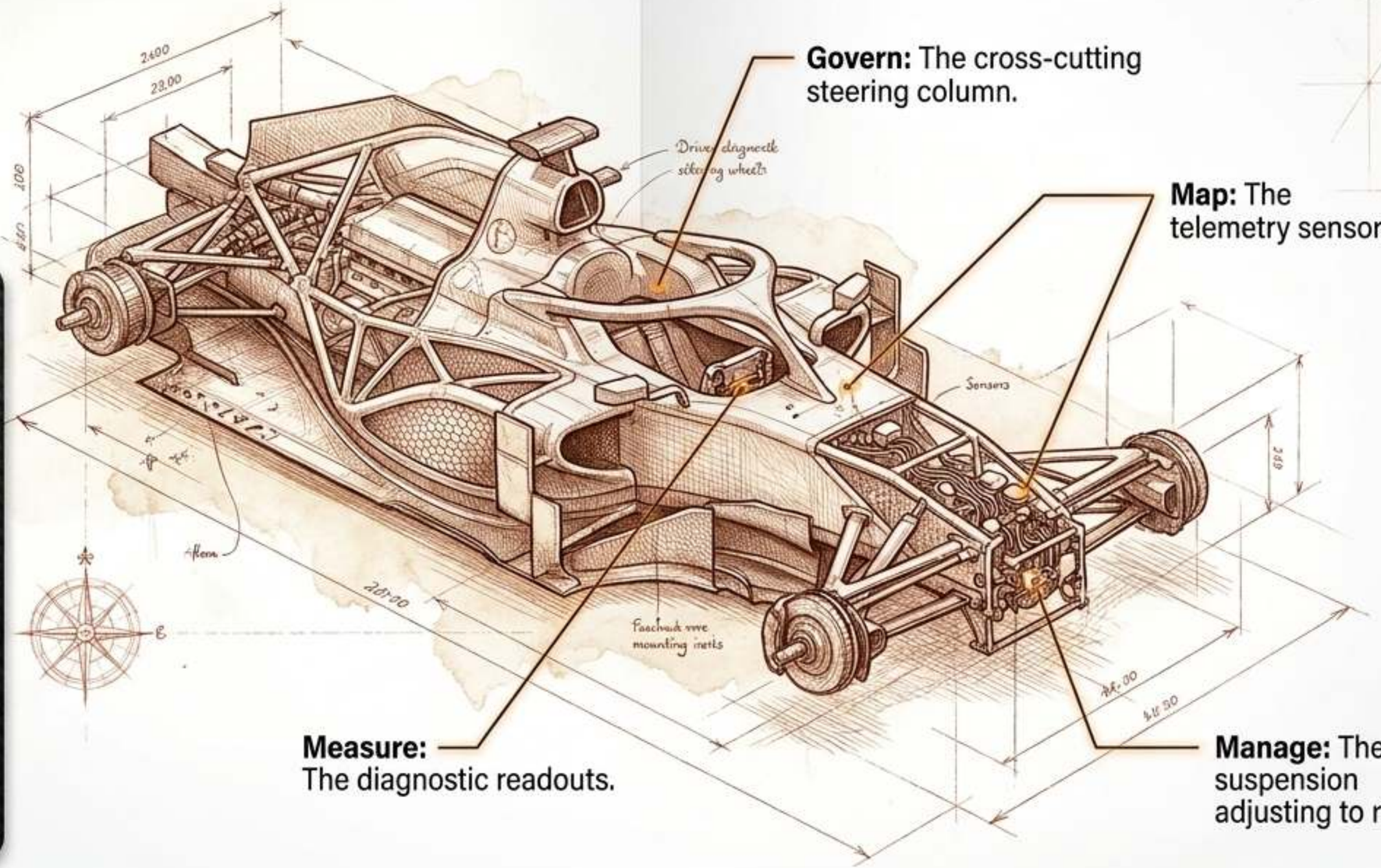
ISO 42001 certification becomes the baseline expectation for enterprise sales.

Shadow AI Weather Warning

- 77% of employees use Gen AI, but only 28% of organizations have policies.
- Non-adoption of governance creates shadow AI breaches costing an additional $650k+ per incident.

Engineering the Chassis: NIST AI RMF 1.0

- Voluntary, lifecycle-based, sector-agnostic structure.
- Cross-walks perfectly to ISO 42001 and the EU AI Act.
- **Core Function:** Manages risks to people, organizations, and ecosystems.



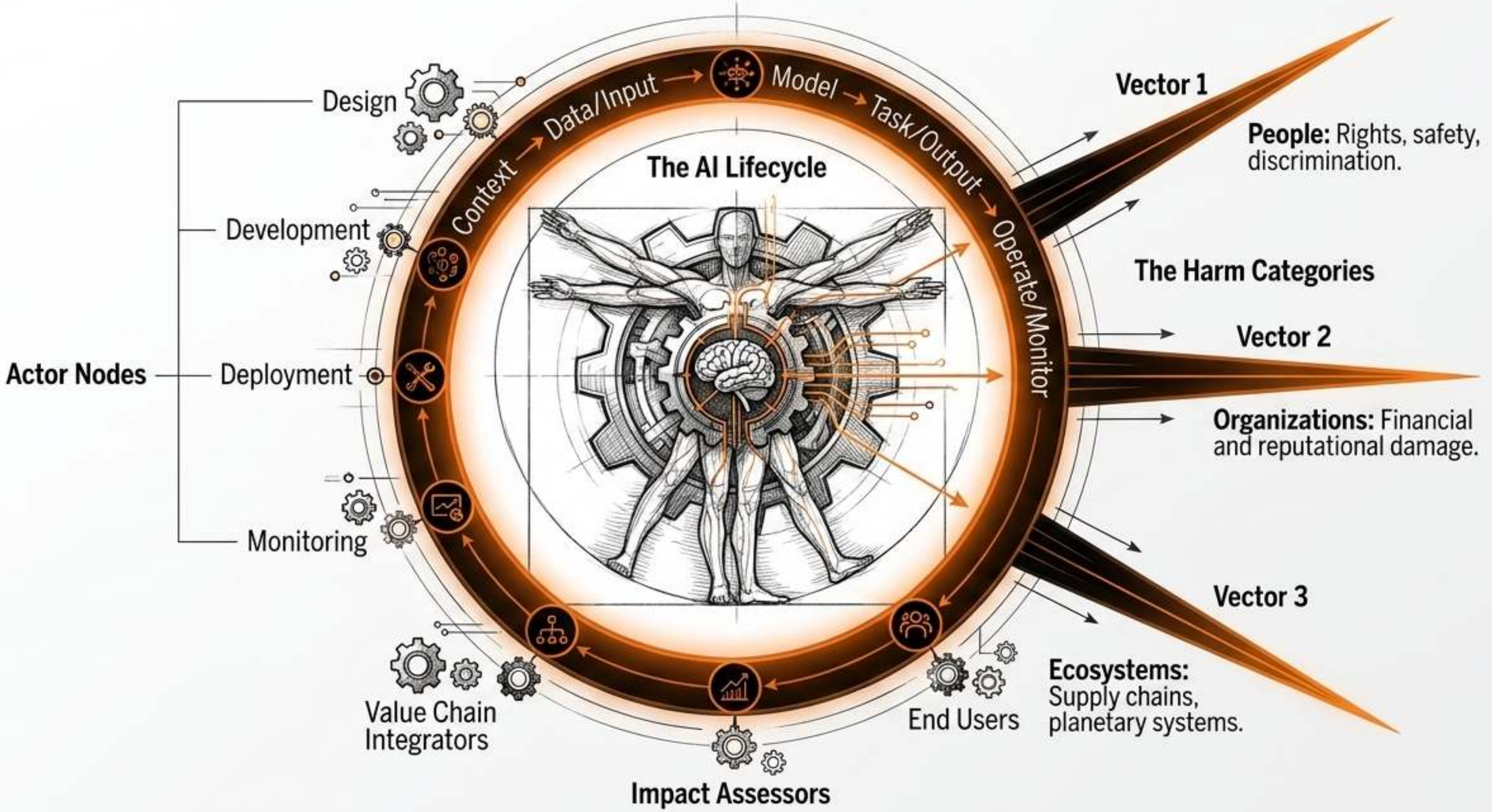
Govern: The cross-cutting steering column.

Map: The telemetry sensors.

Measure: The diagnostic readouts.

Manage: The active suspension adjusting to risks.

Anatomy of an Agentic System



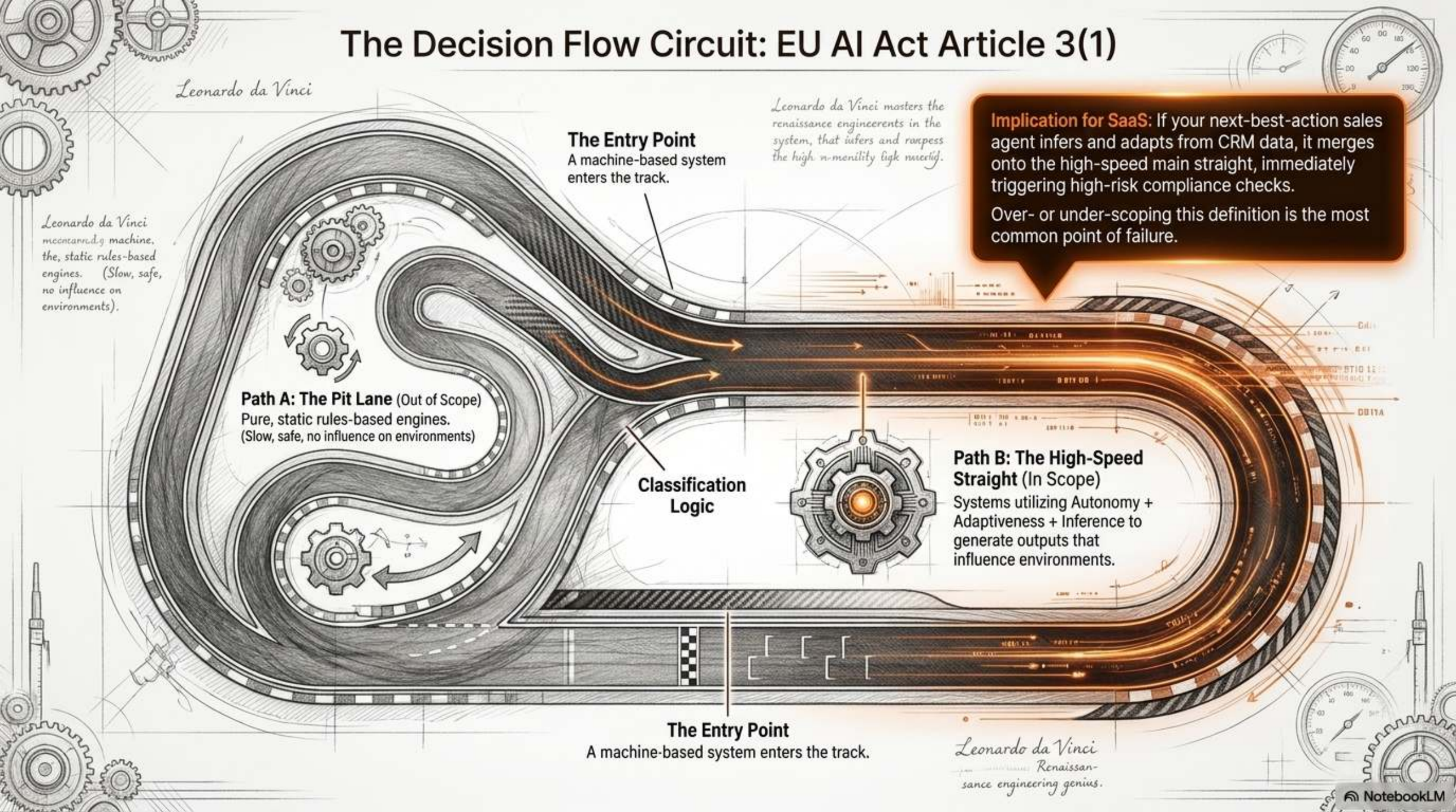
The Trustworthy Telemetry Grid



The Performance Uplift

- Govern is not optional. It requires executive-owned human-in-the-loop gates and continuous TEVV (Testing, Evaluation, Verification, Validation).
- High performers (only 6% of the market per McKinsey) execute this continuous telemetry and capture a massive 39% EBIT impact.

The Decision Flow Circuit: EU AI Act Article 3(1)



NotebookLM

Aerodynamic Drag and Risk Tiers



Top Stream

Unacceptable / Prohibited

Turbulent drag. Social Scoring and Subliminal Manipulation. (A wall: you cannot pass).

Middle Stream

High-Risk / Annex III

Requires specific wing adjustments (controls) and Article 6(3) derogation documentation.

Domains: Employment, Essential services (credit), Biometrics, Critical infrastructure, Education, Law enforcement, Migration, Justice.

Limited / Minimal Risk

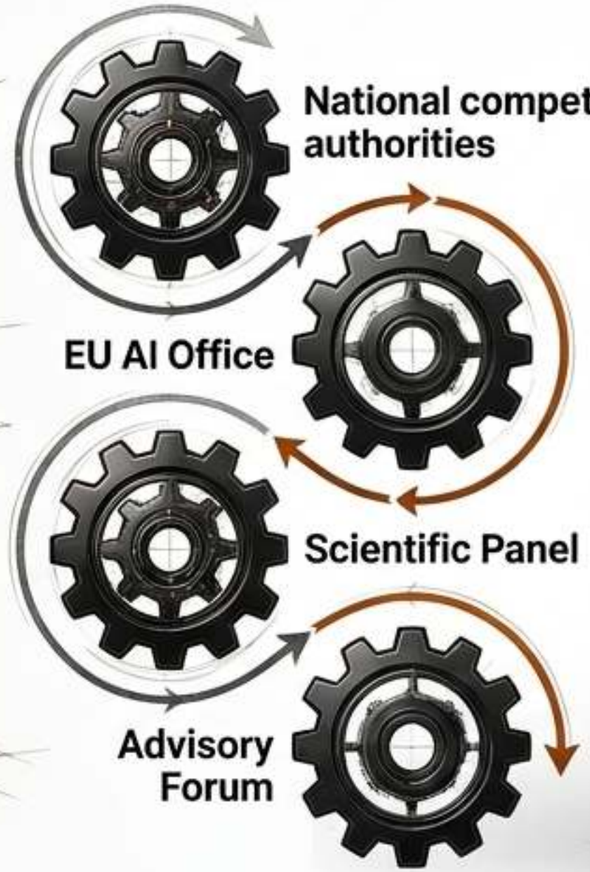
Requires only transparency obligations.

Practitioner Insight: Agentic sales prioritization that influences hiring or credit decisions falls squarely into high-risk under employment/essential services.

Leonardo da Vinci

Renaissance engineering genius

The Crash Barrier: Enforcement and Penalties



Effective Aug 2026

- **Prohibited practices:** €35M or 7% global turnover (whichever is higher).
- **High-risk / Operator obligations:** €15M or 3% global turnover.
- **GPAI models:** Up to 3% or €15M.
- **Misleading information:** €7.5M or 1% global turnover.

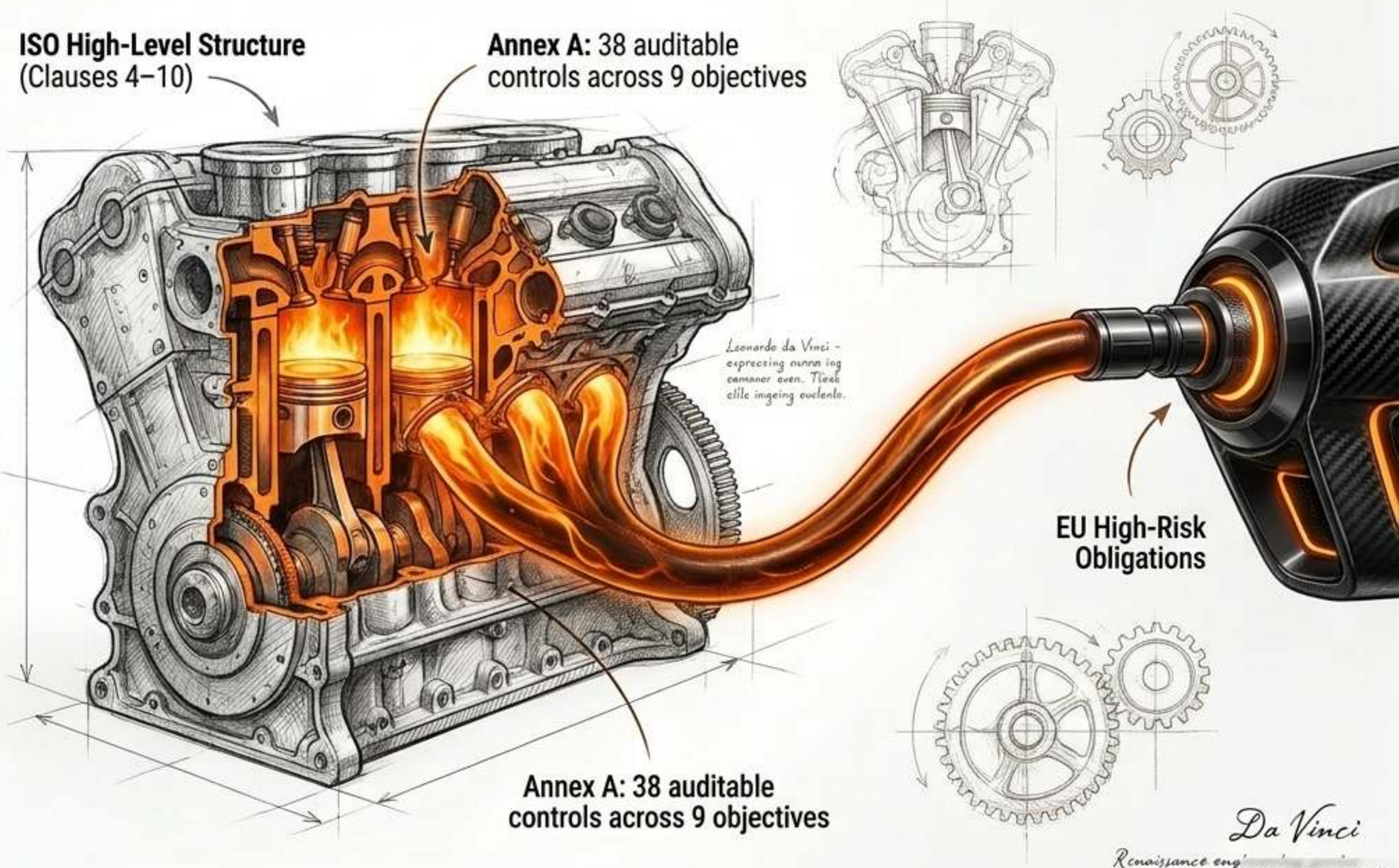
For a $500M ARR SaaS company, a single prohibited violation means €35M+ in fines. Sophizo's classification playbook prevents clients from ever seeing these numbers.

Da Vinci

ISO 42001: The Certifiable AI Engine

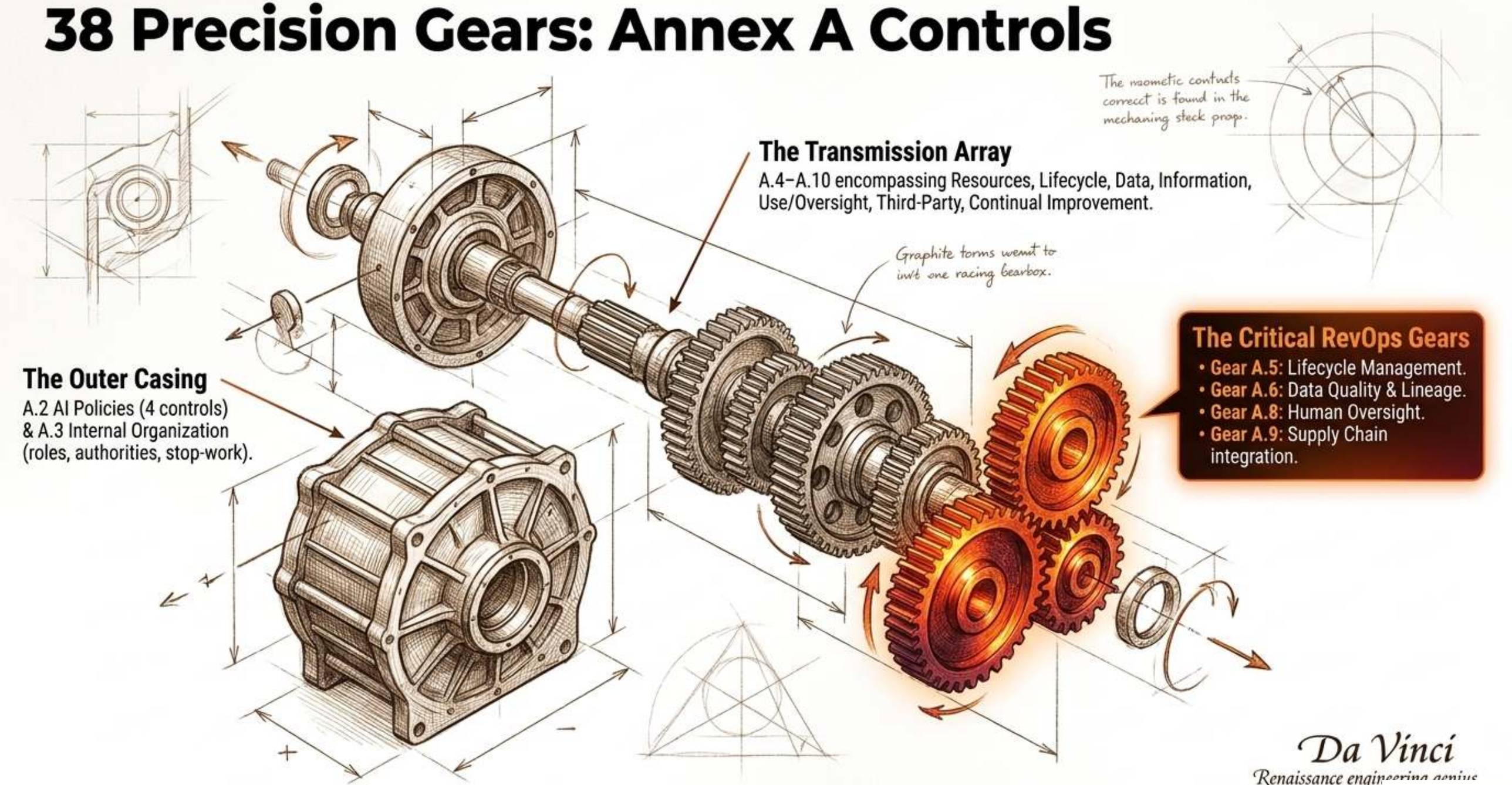
The Investment Reality

- Certification costs $250k–$350k over 3 years for mid-sized firms.
- **The ROI**: Pays for itself in dramatically faster sales cycles, avoided security incidents, and signaling elite maturity to customers, regulators, and investors.



NotebookLM

38 Precision Gears: Annex A Controls



Master Telemetry: The Unified Governance Framework



Insight: One unified visual dashboard replaces three separate, expensive audits. This leverages McKinsey high-performer levers (workflow redesign, executive ownership) into a single operational interface.

Da Vinci
Renaissance engineering genius

Apex Cornering: The ROI of Governance

The Cost of Poor Handling

- **AI compliance failures:** $4.4B industry losses in 2025.
- **Shadow AI breach premium:** +$650k–$670k per incident.
- **EU fine exposure:** up to €35M / 7% turnover.
- **ISO non-certification:** Lost enterprise contracts, stalled sales.



The Governance Accelerator Lift

- **3× Faster:** GTM approval velocity.
- **18% Lift:** Pipeline velocity acceleration (based on anonymized Sophizo client data).
- **Result:** Governance is revenue insurance that pays for itself in the first closed deal.

Da Vinci
Renaissance engineering genius

The 90-Day Engineering Sprint: Sophizo Accelerator

Pit Stop

Sector 1 (Weeks 1–2):

EU Classification + NIST Actor/Harm Register. (Diagnostic phase).

Sector 2 (Weeks 3–6):

ISO Annex A gap analysis + evidence dashboard. (Structural engineering).

Sector 3 (Ongoing):

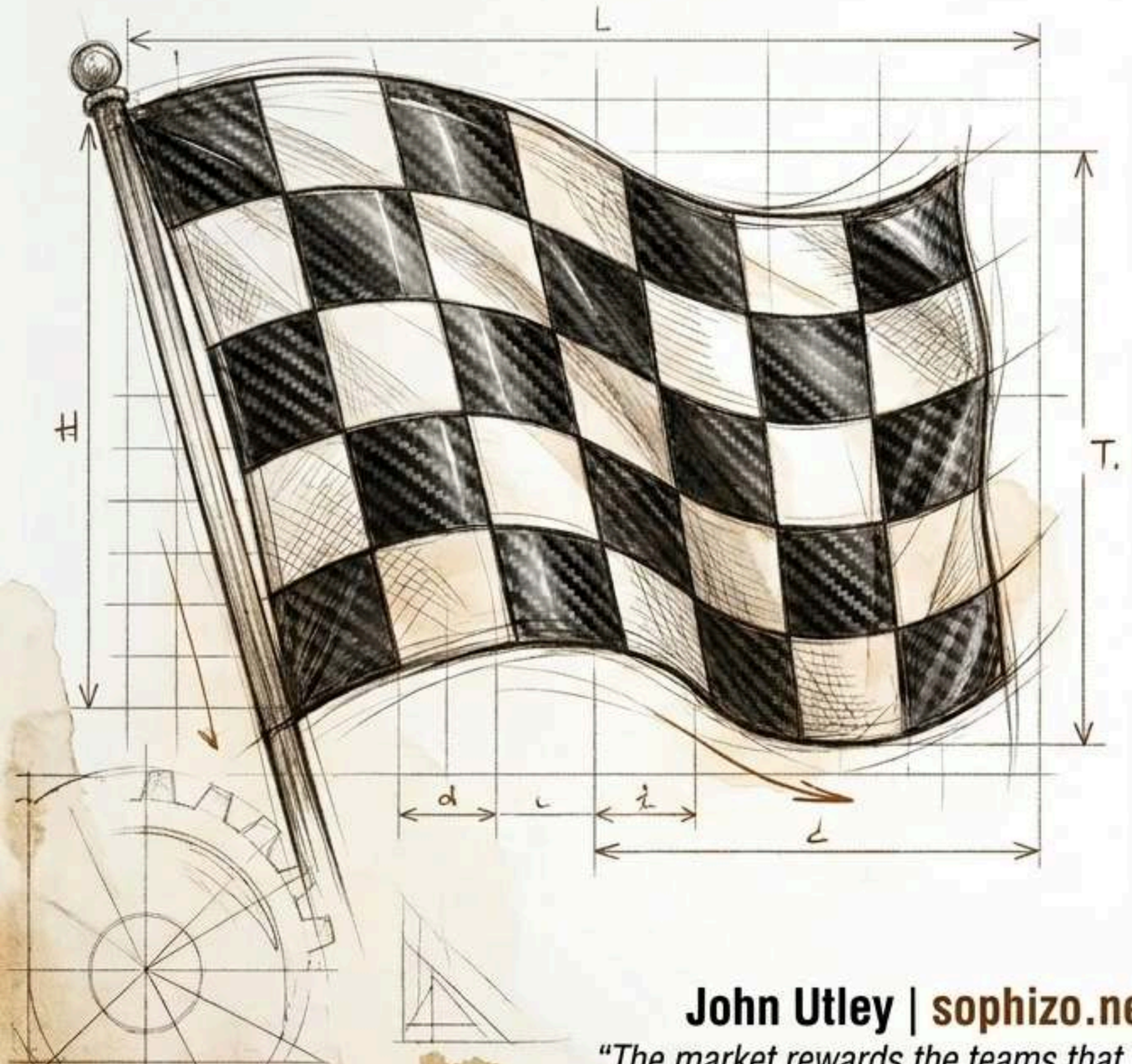
Embedded controls integrated directly into ForecastIQ and the broader RevOps stack. (Live telemetry).

Deliverables & Investment

- Playbooks, templates, and live monitoring.
- **Investment**: $45k–$75k + optional continuous fractional retainer.

Da Vinci
Renaissance engineering genius

Take the Checkered Flag



1. Map Your Risk: Book a 30-minute Classification Diagnostic.

2. Download the Blueprint: Access the EU Checklist + NIST Template + ISO Scorecard.

3. Engage the Engine: Sophizo acts as your Fractional AI Officer, shipping revenue while de-risking the entire enterprise.

John Utley | sophizo.net/governance-accelerator

"The market rewards the teams that implement, not just talk about, controls."

Da Vinci
Renaissance engineering genius