



# The Algorithmic Liability Crisis

Global governance gaps are leaving enterprises dangerously exposed as AI deployment outpaces legal frameworks.

2025 RISK BRIEFING

## The Stakes

# A Crisis Hidden in Plain Sight



Organizations are deploying **opaque** "black box" AI into high-stakes sectors — healthcare, finance, public safety — without adequate risk guardrails.

The WEF defines this moment as an "**age of competition**": deep geopolitical fragmentation, systemic risk, and legal frameworks that have not kept pace.

- ❏ Legal liability blind spots are now among the most critical enterprise vulnerabilities.

# The "Death by AI" Liability Crisis

**2,000+**

**Legal Claims by 2026**

Gartner's projected "death by AI" cases — a threshold we are on track to exceed

**2x**

**Claims Doubling by 2029**

AI-related legal actions are projected to double from the previous decade

**\$15T**

**AI-Intermediated B2B Spend**

90% of B2B buying by 2028 — autonomous machine-to-machine transactions, liability at scale

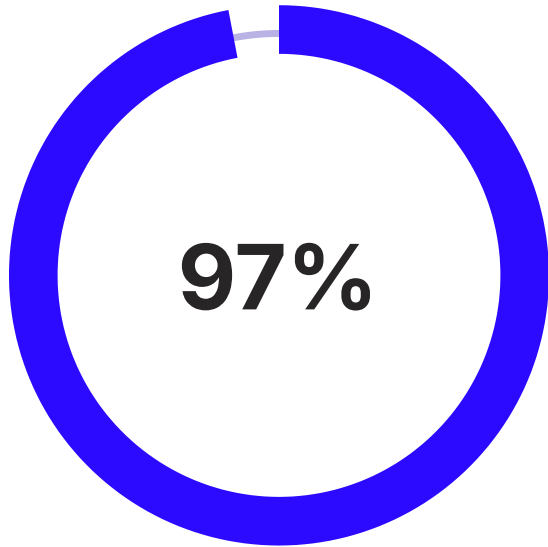


## When Machines Transact, Who Is Liable?

By 2028, **90% of B2B procurement** will be intermediated by AI agents. As machine-to-machine deals execute autonomously, liability risks scale exponentially — with no human signature on the dotted line.

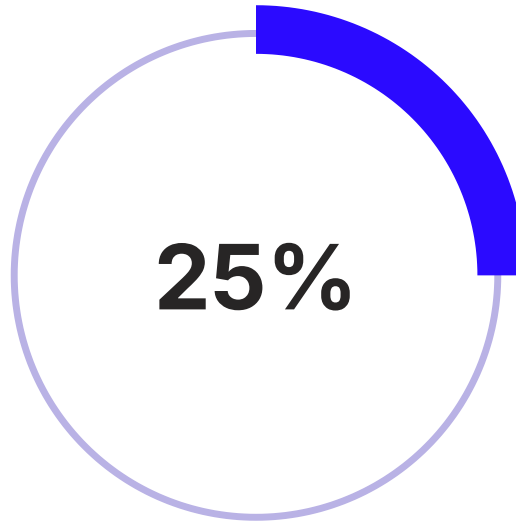
# The Governance Execution Gap

This is not a lack of awareness. It is a **failure of execution.**



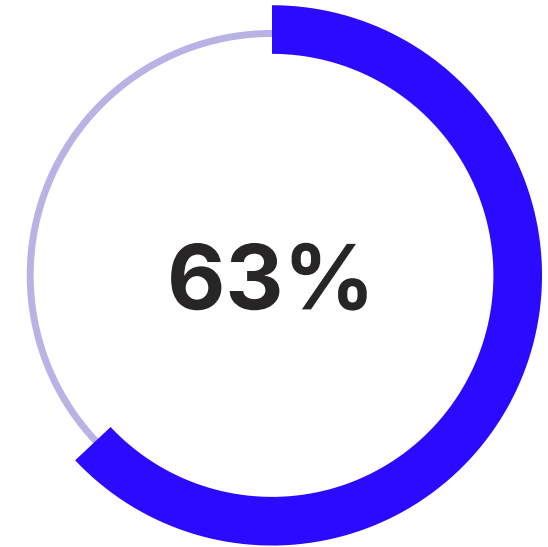
## Breached Without Controls

of AI-related breach victims lacked proper access controls



## Full Governance Implemented

Only a quarter of organizations have fully deployed AI governance programs



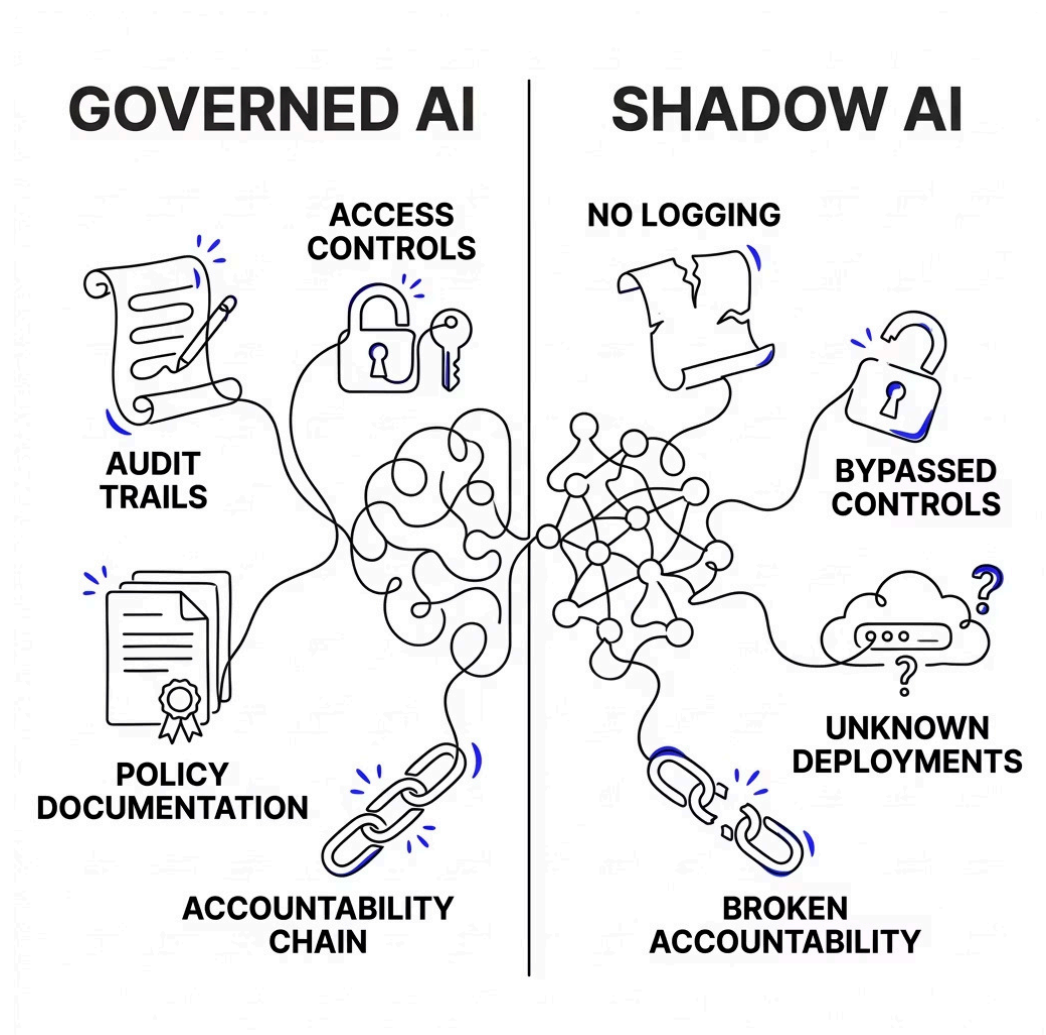
## No Policy at Breach Time

of breached organizations had no formal AI governance policy in place

# Shadow AI & Vanishing Accountability

The presence of **shadow AI** – unauthorized models operating outside governance frameworks – combined with absent audit trails makes it nearly impossible to establish a clear chain of accountability when systems cause harm.

- No logs, no liability defense
- Rogue deployments bypass policy controls
- Regulators demand answers enterprises cannot provide



CHAPTER 3

# Macro Context: Geoeconomic Confrontation

The WEF Global Risks Report 2026 ranks **Geoeconomic Confrontation** as the #1 global risk — for both the current year and the two-year horizon.



# The Expanding Risk Zone

## **Military AI Escalation**

Rapid advancement and expanding military AI applications raise the specter of unintended, rapid conflict escalation.

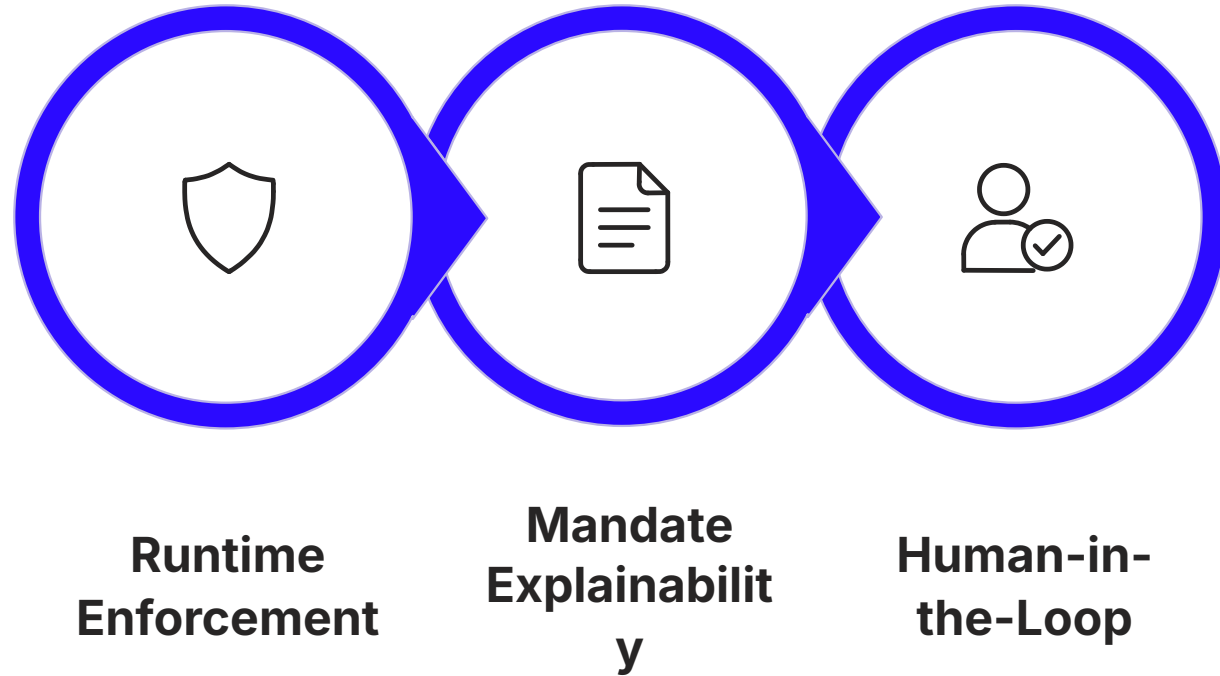
## **AI-Driven Disinformation**

Misinformation erodes shared facts and institutional trust — a corporate AI failure can quickly become a societal crisis.

## **The Polycrisis Threat**

A geopolitical conflict disrupting supply chains *simultaneously* with an AI cyberattack overwhelms traditional crisis protocols.

# Three Non-Negotiable Actions



Point-in-time audits are no longer sufficient. Mature organizations embed governance at every layer — from model design to real-time enforcement to human oversight.

## Action 1: Runtime Enforcement

Deploy AI governance platforms that enable **continuous monitoring and automated policy enforcement** — catching anomalies before harmful actions execute.

- ❏ Static audits are a relic. Runtime enforcement is the new baseline.

## Action 2: Mandate Explainability

Implement **AI explainability, ethical design, and transparent data provenance** as non-negotiable legal shields against black-box liability.

- ❏ If you can't explain a decision, you can't defend it in court.

## Action 3: Human-in-the-Loop

Despite pressure for full autonomy, the most mature organizations maintain **strict HITL validation** for high-stakes decisions — ensuring humans retain ultimate oversight and legal accountability.



# The Bottom Line

## **Liability is Accelerating**

2,000+ "death by AI" claims by 2026.  
\$15T in autonomous transactions by 2028. The clock is running.

## **Governance Gaps Are Measurable**

Only 25% of organizations are fully ready. 97% of breach victims lacked basic controls. These are choices, not accidents.

## **Act Now or Absorb the Risk**

Runtime enforcement, explainability, and HITL are not optional — they are your legal and operational lifeline.