



Next-Gen Cyber GRC: Predictive. Unified. Agentic.

June 9, 2025

Management Team

30+ years experience building
and scaling AI systems



CEO & Founder
Nosa Omoigui



GTM
Chad Holmes



Chief Marketing Officer
Lisa Kalscheur



Customer Success
Sasha Tuel



Customer Success
Kimberly Padley



Front End Development
Stephen Madson

Board and Advisors



Chairman
Nosa Omoigui



Board Member
Chuck Cory

*Former Global Chair,
Technology Investments
(30+ years)*

Morgan Stanley



Board Member
Gary Rubens



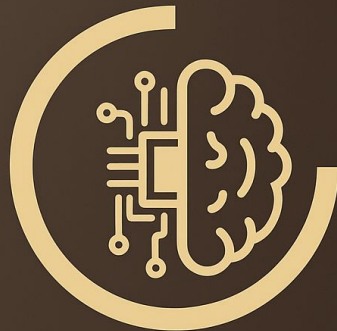
Strategic Advisor
John Bellizzi



Fast Becoming the Standard for AI-Powered Cyber GRC



Industry Recognition



Chartis
RiskTech
AI50 2025

One to Watch



Category Winner

One to Watch

Why Cyber GRC in 2025 Feels Different

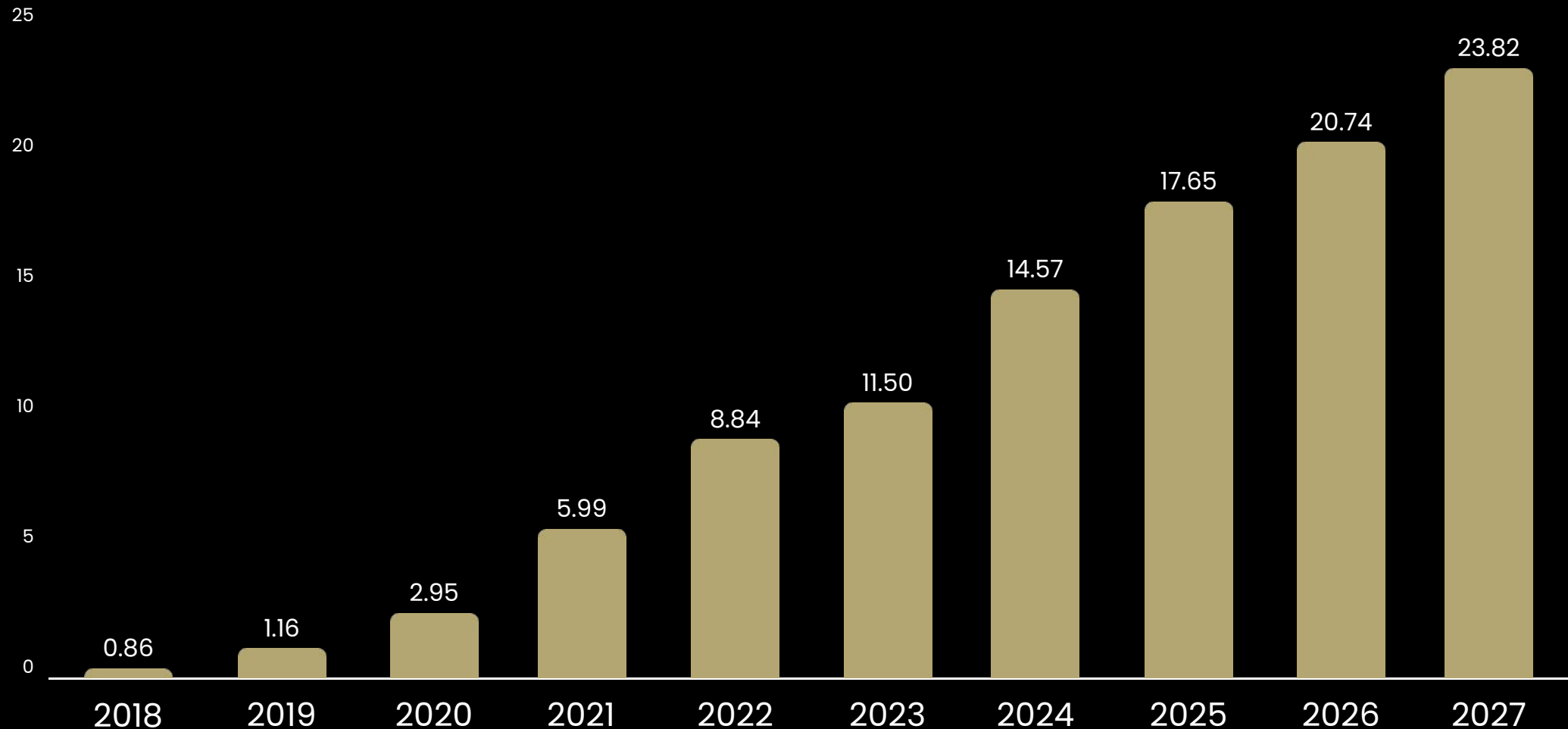
Torrid Regulatory Pace

Rapidly Shifting
Cyber Threat
Landscape

Board-Level Stakes

Cyber risk is growing exponentially

Estimated cost of cyber-threats worldwide (in trillions of dollars)



Industry Leaders Sound Alarm on Hyperconnected Cyber Threats

J.P.Morgan

JPMorgan Chase CISO warns software industry on supply chain security

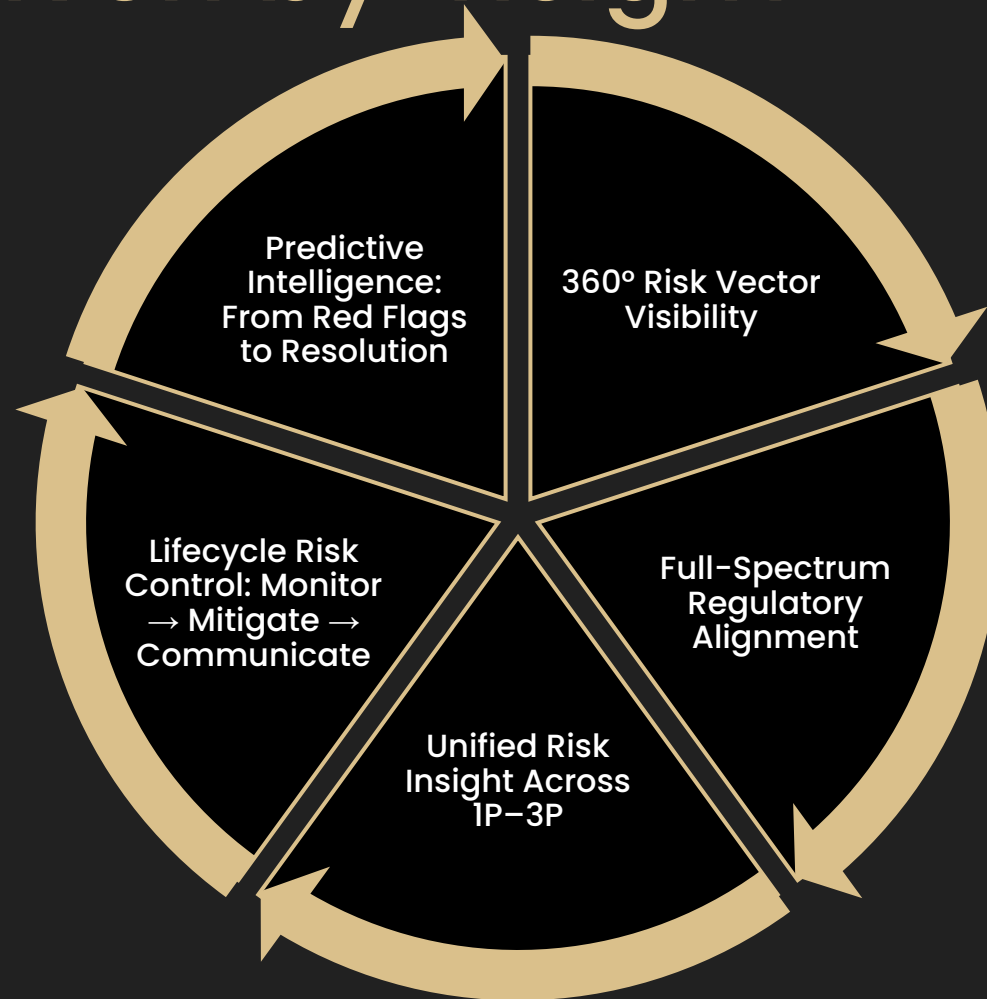
In an open letter, Patrick Opet said third-party vendors need to embrace secure development practices over speed to market.

Published April 28, 2025



“[Today’s IT delivery models] magnify the impact of any weakness, outage, or breach, creating single points of failure with potentially catastrophic systemwide consequences. This fundamental shift demands our collective immediate attention.”

Next-Gen Cyber GRC – Powered by Agents. Driven by Insight



AI-Enabled Coverage of NYL's Core Regulatory & Risk Frameworks

	<p>NYDFS Cybersecurity Regulation (23 NYCRR 500)</p>	<p>Covers enterprise-wide cyber risk governance, third-party risk, board oversight, and incident response – high relevance due to NYL's domicile and data governance mandate.</p>
	<p>NAIC Own Risk and Solvency Assessment (ORSA) Model Act</p>	<p>Ensures firms hold enough capital to meet their obligations to policyholders while promoting strong governance, transparency, and enterprise risk management.</p>
	<p>IFRS 17</p>	<p>Governs how insurance contracts are reported, aiming to increase transparency and comparability. It requires insurers to recognize revenue and profit, aligning financial reporting with the underlying economics of insurance obligations.</p>
	<p>NAIC Cybersecurity Model Law</p>	<p>National guidance aligned with NYDFS cyber rules but broader for multi-state operations.</p>
	<p>NYDFS Regulation 187 (Suitability & Best Interest for Life/Annuities)</p>	<p>Directly impacts product design, distribution risk, and controls – especially for foundational and AARP business.</p>
	<p>Basel III</p>	<p>Strengthens the capital adequacy, liquidity, and risk management of banks and certain large insurers. It ensures institutions maintain sufficient high-quality capital to absorb shocks, reducing the risk of financial system instability.</p>
	<p>NIST AI Risk Management Framework (AI RMF 1.0)</p>	<p>National framework for AI risk controls, transparency, explainability, and bias mitigation – maps well to NYL's enterprise AI governance function.</p>
	<p>IAIS Insurance Core Principles (ICPs)</p>	<p>Global standard for supervisory expectations, risk controls, and governance – relevant to NYL's international business and potential G-SII considerations.</p>
	<p>COSO ERM Framework</p>	<p>Widely used for risk control and governance structure; aligns with ORSA and enterprise risk functions.</p>
	<p>SEC Investment Adviser and ESG Regulations (for NYLIM)</p>	<p>Material for investment arm – covers marketing rules, liquidity risk, and ESG disclosure practices.</p>

Unified Risk Insight (1P-3P)

First-Party Risks (Internal)

- Employees
- Business lines
- Internal systems
- Governance & strategy
- Compliance failures

Second-Party Risks (Affiliates & Close Partners)

- Subsidiaries
- Joint ventures /
co-branded
partnerships
- Intercompany exposure
- Step-in risk
- Weaker affiliate controls

Third Party Risks (External)

- Vendors & outsourcers
- Counterparties
- Correspondent entities &
agents
- Regulatory changes
- Cyber supply chain
threats

From Red Flags to Resolution

Actionable Outputs:



**From Red Flags
to Resolution**
Stakeholders:

Board Risk
Committee

Audit
Committee

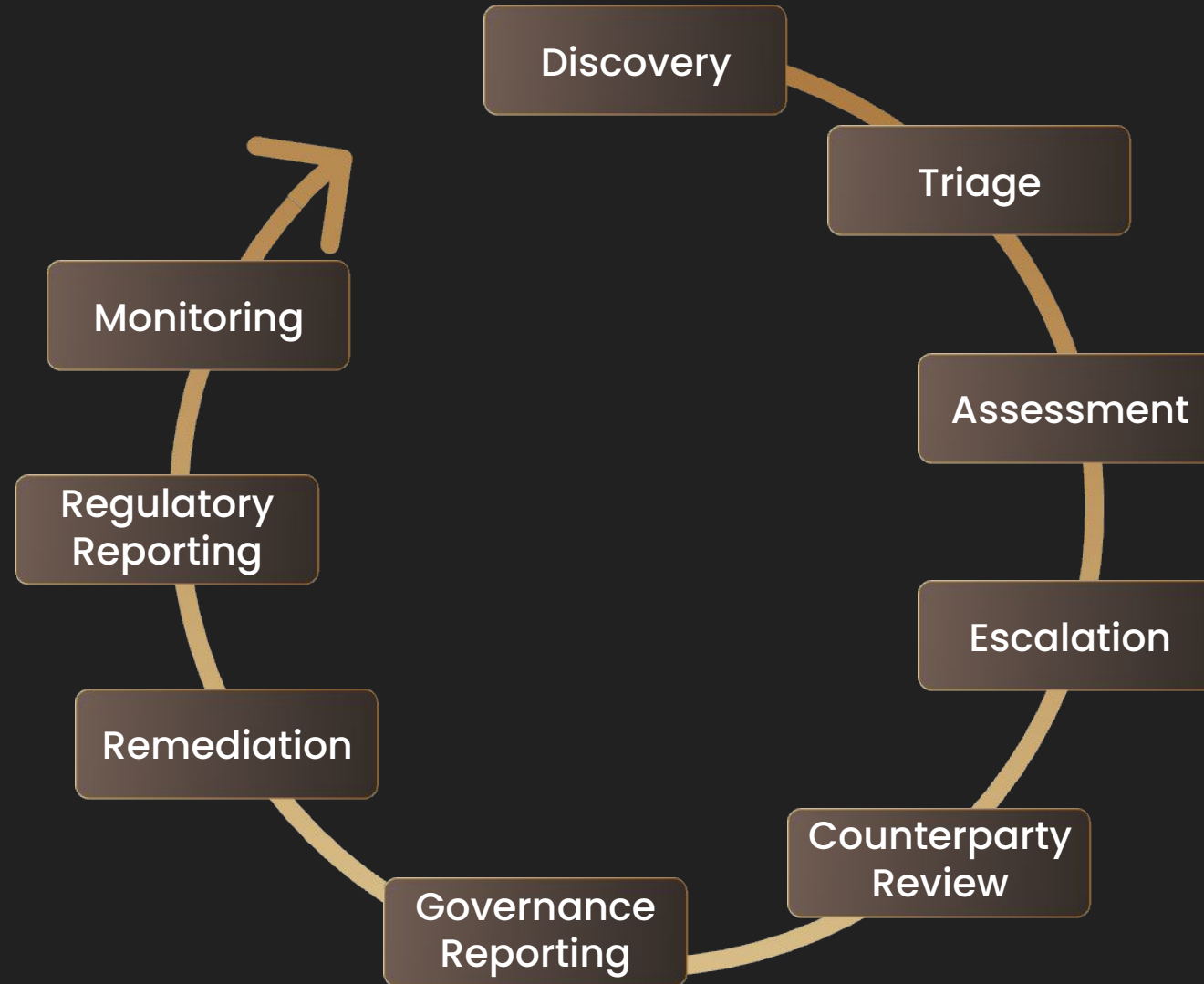
Regulators
(FCA, PRA, EBA, Fed,
NYDFS, etc.)

Line Of
Business Heads

Risk And
Compliance
Officers

Internal Audit

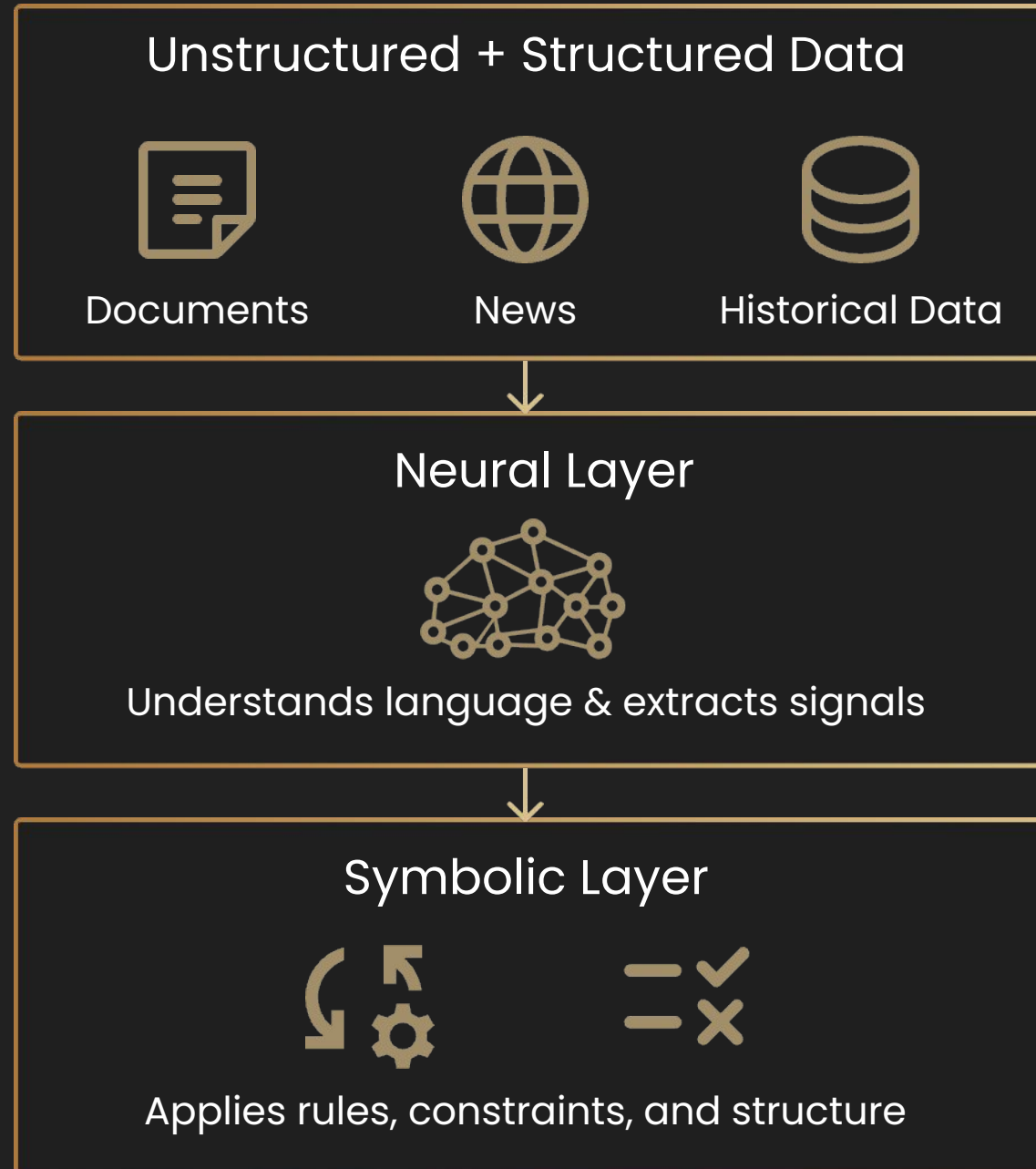
Agentic Risk Management Lifecycle



How Weave.AI works

Why Neuro-Symbolic AI Matters

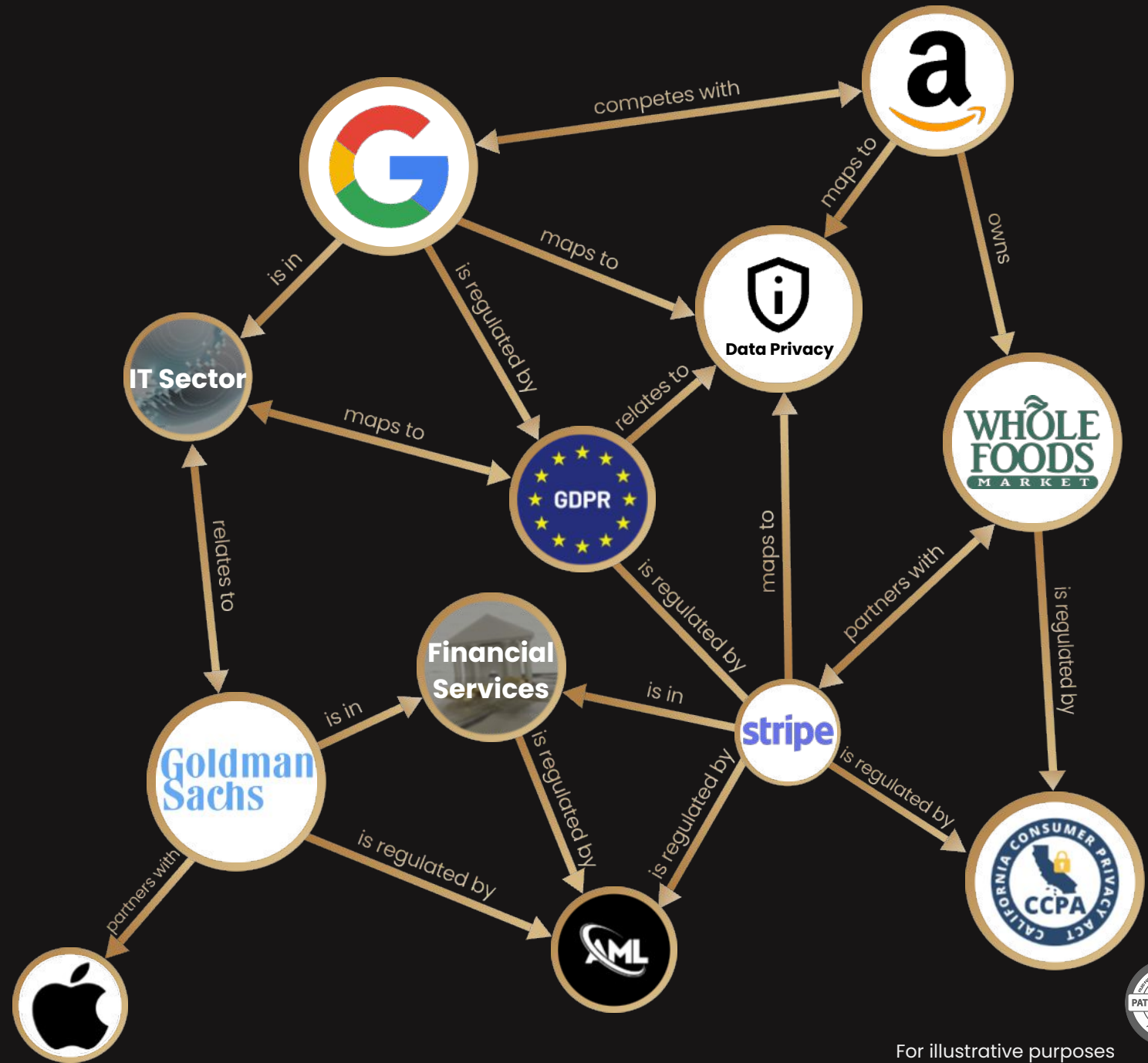
- Traditional LLMs generate fluid but unverified outputs
- Neuro-symbolic AI ensures every insight is grounded
- The knowledge graph maps critical relationships
- Outputs are **traceable**, **defensible**, and **auditable**



The Weave.AI Knowledge Graph

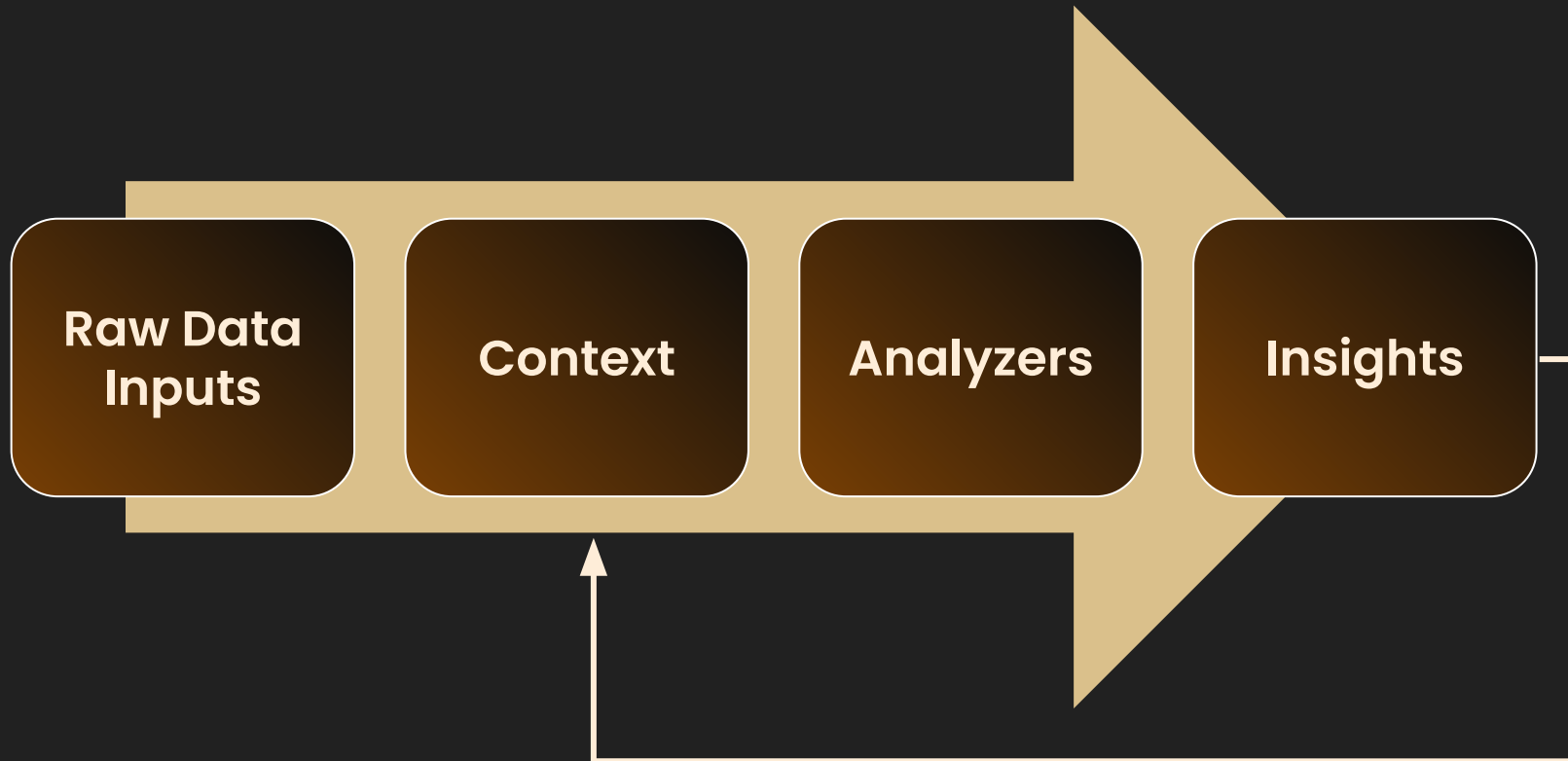
Proprietary Context Engine for Enterprise-Grade Insight

- ✓ Fluent + grounded
- 🛑 No hallucinations or guesses
- 🌐 Knowledge graph links regulations, risks, peers, and internal data
- 📍 Every output is traceable to the source, auditable, and defensible



For illustrative purposes

How Weave.AI works



Unique Insights



Unknown unknowns



Red flags



SWOT analysis



Next best actions



Tailored guidance
On how to plug gaps



Alarms
Predictive alerts



Gap analysis
Specific compliance and
mitigation gaps



Early warning alerts
Emergent risks



Recommendations



Agents
Aligned with regulations
and risk frameworks



Beacons
Agent orchestration
(smoke detectors)

Business Value & ROI

Reduce Risk Exposure

- Identify emergent unknown unknowns & red flags
- Detect control failures before they escalate

Strengthen Compliance & Audit Readiness

- Pinpoint compliance gaps
- Plug gaps with tailored, actionable guidance

Improve Decision Velocity

- Get clear next-best-actions
- Triage and prioritize risk responses



Enhance Risk Visibility & Governance

- Continuous early warnings across 1P/2P/3P risks
- Agentic coverage mapped to regulatory frameworks

Drive Operational Efficiency

- Automate analysis and escalation workflows
- Reduce manual effort and audit cycle time

Quantifiable ROI

- Lower cost of compliance
- Fewer fines, faster remediation, stronger risk-adjusted performance

The Future of Risk Governance Starts Here



- You always know where you stand on the cyber regulations and frameworks that matter
 - NIST, ISO 27001, DORA, and more
- You know if you are following best practices aligned with your peers
 - Spanning first-party, vendor, supplier, and counterparty risk exposure
- You understand the actions you need to take – how, what, when and why
- You can track it all in one view, one place, whenever you want

*See around corners and discover the
'unknown unknowns'*

