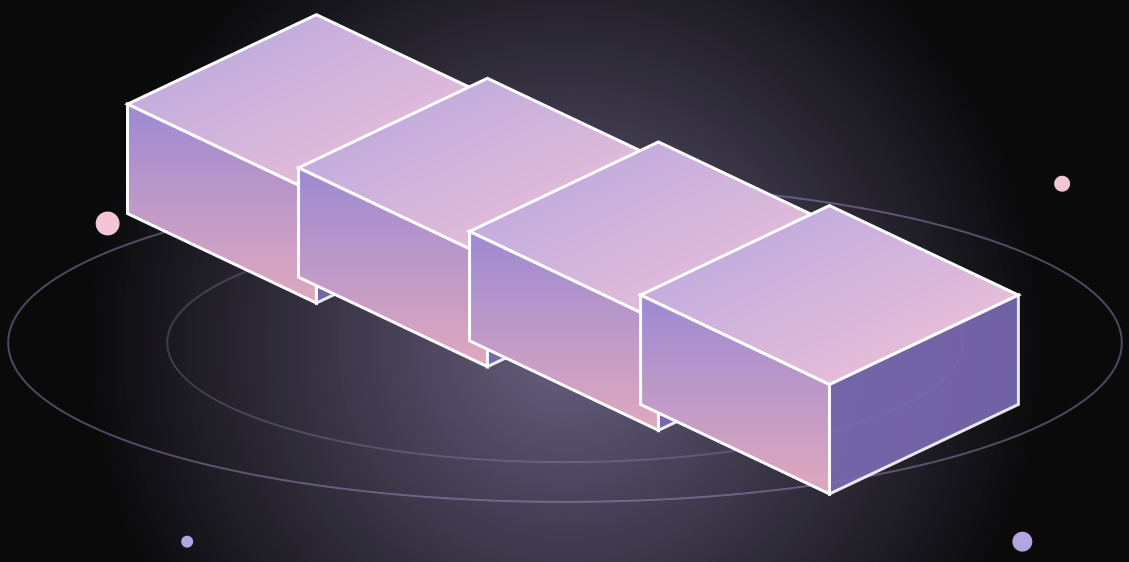
ENTERPRISE BUYER'S GUIDE · 2026 EDITION

The Enterprise Buyer's Guide to AI Governance Platforms

A practical evaluation framework for the leaders responsible for choosing an AI Governance platform — covering capabilities, vendor questions, business case, and buying committee dynamics.

EU AI Act · NIST AI RMF · ISO 42001 · Agentic AI Governance



What's Inside

An eight-chapter walk-through of how to evaluate, select, and build the business case for an AI Governance platform in 2026.

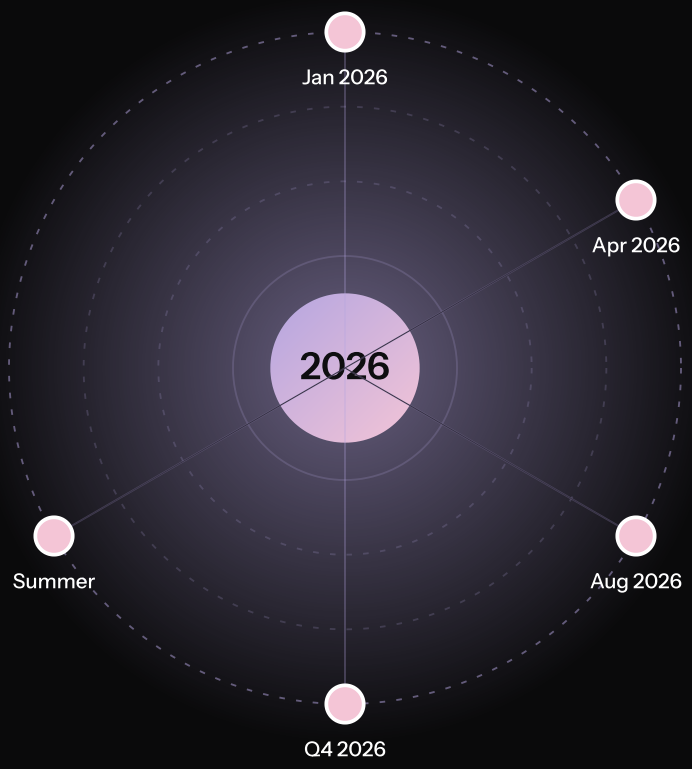
About This Guide

This buyer's guide is based on the 2026 State of AI Governance Report (n=371 practitioners), analyst research from Forrester, Gartner, and IDC, and Credo AI's experience working with Global 2000 enterprises across financial services, healthcare, government, energy, and retail.

Chapter 01 • Why Now

Why AI Governance Matters Now

Three forces have converged in 2026 to make AI governance not just important — but urgent. Agentic proliferation, regulatory pressure, and competitive dynamics all point in the same direction.



Three forces have converged in 2026.

Organizations that build governance capability now will be the ones that can move decisively as requirements become mandatory.

Agentic AI Proliferation

- 33% of enterprise apps include agentic AI by 2028 (Gartner)
- Agents take autonomous actions — not just produce outputs
- Multi-agent chains create untraced accountability gaps
- Shadow agents proliferating in Salesforce, Copilot, Slack
- A procurement agent authorized to request quotes is NOT authorized to approve purchases — only governance answers this

Regulatory Pressure

- EU AI Act enforces high-risk rules Aug 2, 2026 (GPAI/Art. 50)
- Full penalties — up to 7% of global revenue — from 2027
- Singapore IMDA agentic governance framework: Jan 2026
- NIST CAISI AI Agent Standards: Q4 2026
- US SR 26-2 banking guidance: April 2026

Competitive Pressure

- 60% of enterprises deploying AI at scale
- Only 4% governing AI at scale — most exposed
- Governed competitors deploy AI faster with less risk
- AI governance enables board-level AI confidence
- Governance is an accelerant, not an inhibitor

$2.6–4.4T

Annual global value agentic AI could unlock

MCKINSEY GLOBAL INSTITUTE

40%

Agentic AI projects canceled by 2027 — escalating costs, unclear value, inadequate risk controls

GARTNER

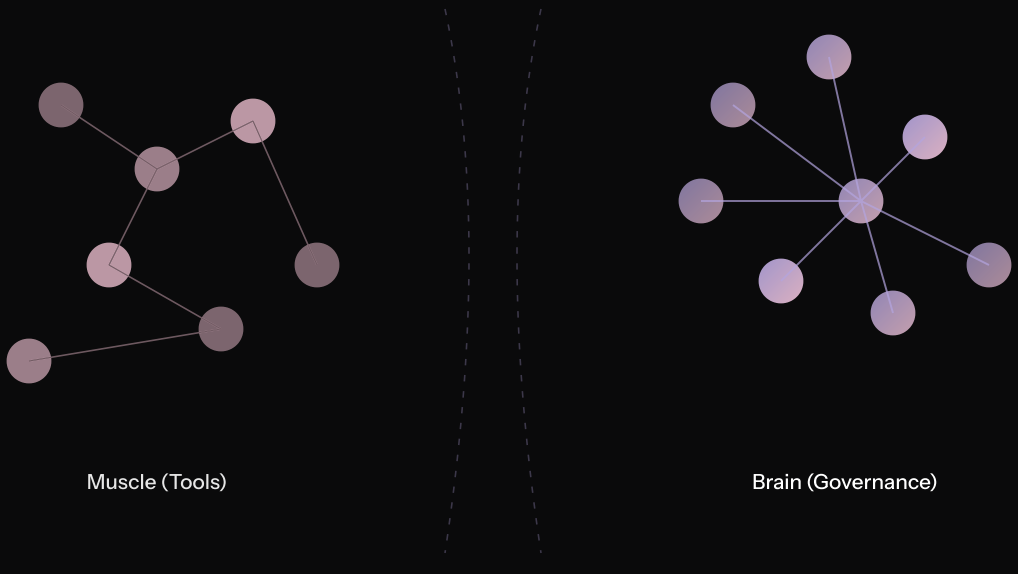
KEY AGENTIC AI REGULATORY MILESTONES

FRAMEWORK	WHAT IT COVERS	DATE
Singapore IMDA	First agentic-specific governance framework: risk bounding, meaningful human accountability	**Jan 2026**
EU AI Act + GPAI	Agentic / autonomous use as systemic risk; Art. 50 transparency + high-risk classification	**Aug 2, 2026**
US SR 26-2 (Banking)	Federal banking agencies guidance on GenAI + agentic AI; interagency RFI forthcoming	**Apr 2026**
NIST CAISI	AI agent security, identity, authorization, auditing, and non-repudiation standards	**Q4 2026**
UK FCA Mills Review	Long-term impact of AI on retail financial services including agentic systems	**Summer 2026**

Chapter 02 • The Landscape

Understanding the AI Governance Landscape

The market is noisy. Runtime security vendors, content safety providers, and observability platforms all claim to 'solve AI governance.' Knowing the difference between governance and the tools it governs is the first step.



Muscle (Tools)

Brain (Governance)

What governance is — and isn't.

The AI governance market is noisy. Runtime security vendors, content safety providers, and observability platforms all claim to "solve AI governance." Understanding the difference between governance and the tools they govern is the first step to a sound evaluation.

These Are AI Tools, Not AI Governance

- × Red teaming and adversarial testing
- × Model evaluation and benchmarking
- × Runtime security and guardrails
- × AI observability and monitoring
- × Content safety / I/O filtering
- × Data privacy management

These tools answer: "Is this agent safe right now?" That is essential. But it is not governance — it is a point-in-time check. Governance requires a system of record that proves, continuously and at enterprise scale, that every AI system is managed appropriately.

This Is AI Governance

- + Enterprise-wide AI inventory and registry
- + Agent cards: sanctioned purpose, config, risk, policies, audit trail
- + Agent constitutions: inviolable behavioral constraints
- + Pre-deployment gate: risk assessed, sanctioned, recorded before any agent runs
- + Runtime governance validating behavior against agent cards
- + Regulatory compliance evidence connected to actual frameworks
- + Accountability structures and ownership models

AI governance answers: "Is our entire AI program managed, auditable, and compliant?" This requires a system above the tools, owned by the accountability owner whose job is on the line if governance fails.

The Governance Intelligence Layer — And Why Agentic AI Raises the Stakes

Enterprise AI governance today means a system of record that is contextual to your specific use cases, continuous across the full AI lifecycle, and comprehensive across all AI systems — built, bought, embedded, and shadow. That is the intelligence layer. For agentic AI, the stakes rise significantly: agents take autonomous actions in milliseconds. External-only governance — quarterly audits, offline risk assessments — is structurally too slow.

For agentic AI, governance must extend into the loop — present in how agents are defined, constrained, authorized, and held accountable continuously. The intelligence layer that governs models today becomes the control plane that governs agents tomorrow.

The Platform Vendor Neutrality Problem

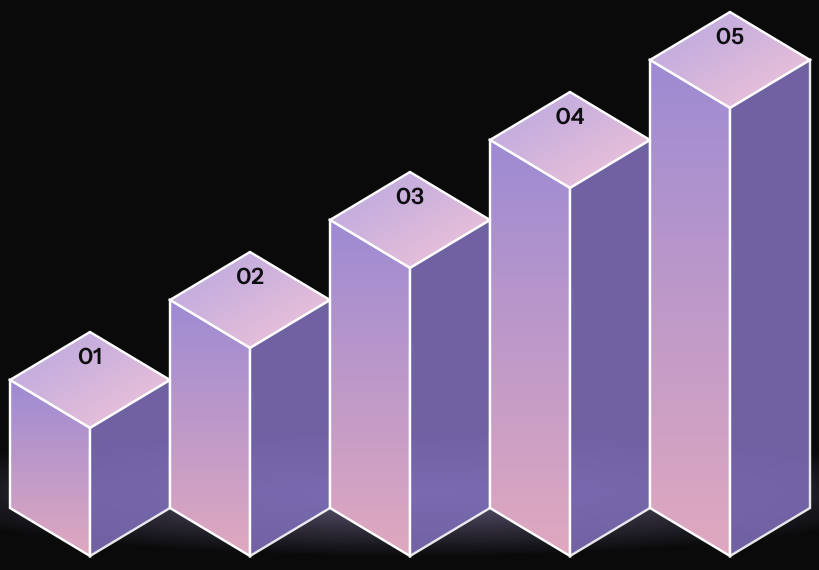
An enterprise needs its governance layer to tell the truth about every agent — including agents built by the platform vendors it depends on. Microsoft cannot be the neutral governance brain for Copilot agents. Salesforce cannot govern Agentforce impartially. A cybersecurity vendor that acquired an observability tool is not positioned to produce the accountability record that comprehensive governance requires.

Trust in governance is only meaningful when the governing entity has no stake in the outcome of what it governs.

Chapter 03 • Evaluation Criteria

5 Capabilities Every Platform Must Have

These five capabilities separate platforms that deliver governance from platforms that create the appearance of it. Any platform missing one is a point tool, not a solution.



The five capabilities that separate platforms from point tools.

Not all AI governance platforms are created equal. Any platform missing these is a point tool, not a governance solution.

01 Universal AI Registry & Discovery — Critical

A complete, live inventory of every AI agent and system in the organization — built, bought, embedded (Salesforce, ServiceNow, Microsoft, Workday), and shadow. If you can't see it, you can't govern it.

+ Must have: Auto-discovery of shadow and embedded agents. Coverage for third-party and agentic AI. Not just models you built.

× Watch for: Manual-only inventory. No shadow AI detection. No coverage of procured or SaaS-embedded AI.

02 Risk Assessment Engine — Critical

Automated, consistent risk classification across all AI system types — ML, GenAI, agentic, and third-party. Assigns risk tiers calibrated to the agent's sanctioned purpose, business context, and applicable regulation.

+ Must have: Agent-specific risk criteria including autonomy level and tool access scope. Agentic AI risk assessment. Regulatory mapping.

× Watch for: One-size-fits-all risk scores. No agentic AI-specific criteria. Risk scores without regulatory mapping.

03 Policy & Compliance Automation — Critical

Pre-built, maintained policy packs for major regulations and frameworks — EU AI Act, NIST AI RMF, ISO 42001, SOC 2 — that stay current as requirements evolve. Connected to actual deployed agents, not living in a PDF.

+ Must have: Pre-built EU AI Act policy pack. Article-level coverage. Policy packs maintained by vendor, not DIY.

× Watch for: Build-your-own compliance. No EU AI Act coverage. Policy framework that requires internal legal team to populate.

04 Agent Card + Pre-Deployment Gate — Critical

A governance-grade record for every agent (sanctioned purpose, constitution, business context configuration, risk classification, applicable policies, accountability owner, and evidence trail) plus a formal gate that must be passed before any agent runs.

+ Must have: Agent cards versioned so any past action can be reconstructed. Formal sanctioning recorded. Pre-deployment gate is programmatic, not an approval email.

× Watch for: No agent card or governance specification per agent. Pre-deployment review is a human checklist, not an architectural gate. Constitutions absent.

05 Audit-Ready Documentation — Critical

Continuous, tamper-evident evidence trail that proves governance happened. Answers any regulatory inquiry before it is asked — not assembled manually during audit season.

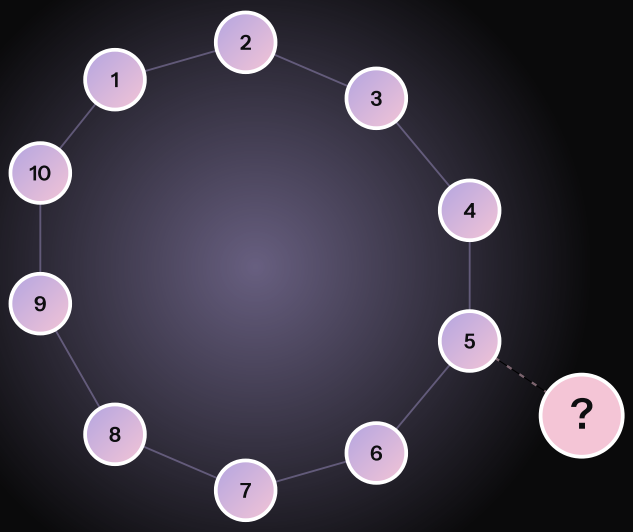
+ Must have: Continuous evidence collection. Tamper-evident audit log. Regulator-ready reports (EU AI Act, NIST format). Reconstructable per-agent history.

× Watch for: Audit documentation assembled manually. No continuous evidence. Reports that require significant manual preparation.

Chapter 04 • Vendor Evaluation

10 Questions to Ask Every Vendor

A diagnostic — not a checklist. Questions 6–10 are the Five Critical Tests for true agentic AI governance. No AI security or observability tool can pass them.



Cut through the marketing language.

Questions 6–10 are the Five Critical Tests for true agentic AI governance. No AI security or observability tool can pass them.

01 Does your platform cover all AI types?

Must cover ML models, GenAI, autonomous agents, and third-party AI. Ask for proof — not just a feature checkbox.

02 How do you handle shadow AI and unregistered systems?

Ask for their discovery methodology. Passive registration is insufficient — you need auto-discovery including agents embedded in SaaS platforms.

03 Show me your EU AI Act coverage — and how often are policy packs updated?

They should have a pre-built policy pack. Ask them to map it live. Then ask: how often is it updated, and how? Credo AI updates continuously. Some platforms update on quarterly or annual release cycles — leaving you exposed to regulatory changes in between.

04 What does your audit trail actually contain?

Ask to see a real audit trail. Confirm it's tamper-evident, continuous (not assembled at audit time), and in regulator-ready format.

05 How does your platform integrate with our existing tooling?

Ask specifically about red teaming results, observability data, and MLOps pipeline integration. Surface-level webhooks are not governance integration.

06 What is your typical time-to-value after implementation?

Ask for median time-to-first-use-case from contract signing. 6+ months is a red flag. GAIA-assisted configuration should reach value in weeks, not quarters.

07 Pre-Deployment Test: Does governance begin before deployment?

If a platform only activates once an agent is running, it is not governing the most consequential decisions. Risk assessment, constitution, sanctioning must all exist before the agent runs.

08 Accountability Record Test: Show me an agent card for any specific agent.

It must include sanctioned purpose, business context config, constitution, risk classification, applicable policies, and evidence trail. If these do not exist in structured form, there is no governance.

09 Policy Connection Test: Does it connect to actual regulatory frameworks?

Not custom thresholds — actual regulatory frameworks (EU AI Act, Singapore IMDA, NIST CAISI). Can they demonstrate connection to each? If not, it is monitoring with governance language applied.

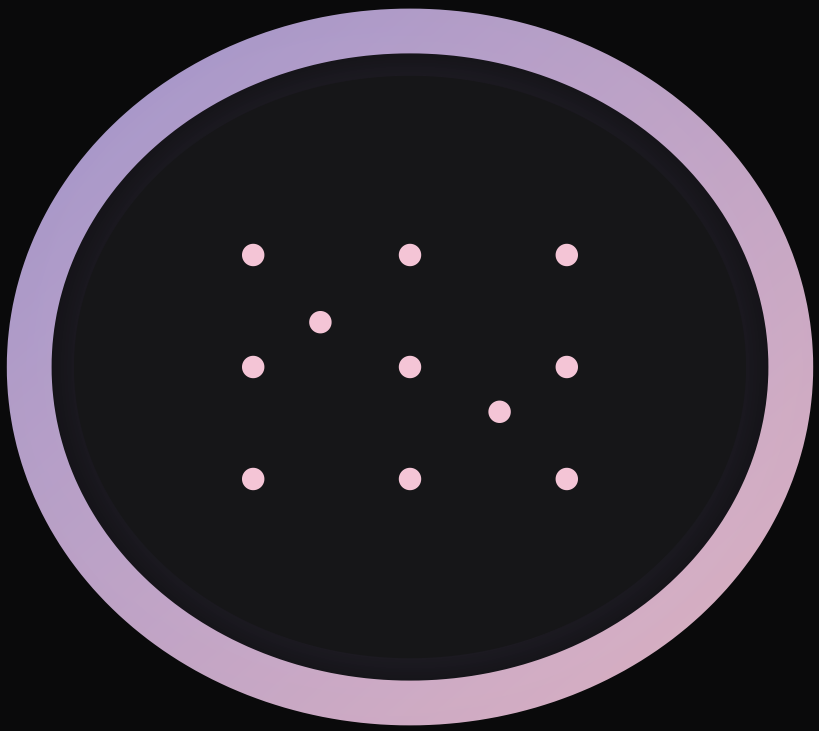
10 Bought Agent Test: Does it govern bought agents, not just ones you built?

Most enterprise deployments involve vendor-built agents in Salesforce, ServiceNow, Microsoft, Workday. A platform that only works when you own the code is not adequate.

Chapter 05 • What You Have

Auditing What You Already Have

Most organizations have significant AI tooling — but very few have the governance brain that ties it all together. Use this chapter to audit your current stack and find your gaps.



Audit your current stack.

Most organizations already have significant AI tooling — but very few have the governance brain that ties it all together.

Tools You Likely Have (Muscle)

Security tooling	Common
MLOps / model registries	Common
AI observability / monitoring	Common
Content safety filters	Common
Data privacy management	Less common
Red teaming tools	Less common

The brain/muscle insight: Muscles without a brain do not know why they are acting, whether a given action is appropriate, or what the organization committed to when it deployed the system. Most tools currently sold as agentic AI governance solutions are excellent muscles being asked to do the work of a brain.

Governance You Probably Lack (Brain)

Enterprise-wide AI registry — built, bought, embedded, shadow	Gap
Agent cards: structured per-agent governance record (purpose, risk, policy, evidence trail)	Emerging
Pre-deployment gate — programmatic review and sanctioning before any agent runs	Emerging
Runtime governance validating behavior against sanctioned scope — not just anomaly detection	Emerging
Pre-built EU AI Act policy pack connected to deployed agents	Gap
Continuous audit documentation — not assembled at audit time	Gap

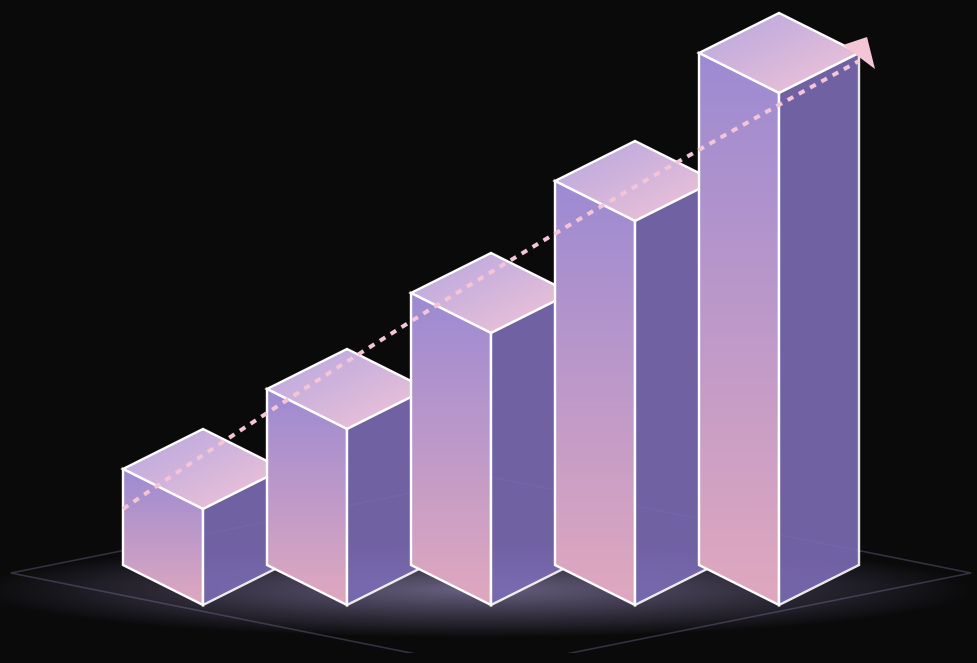
Enterprise Self-Assessment Scorecard

QUESTION	YES	PARTIAL	GAP
Do you have a complete, current inventory of every AI system in your organization — models, GenAI, agents, and third-party AI?	☐	☐	☐
Can you produce EU AI Act documentation on demand for any high-risk AI system, without manual assembly?	☐	☐	☐
Do you have a defined accountability owner for every AI system, documented before deployment?	☐	☐	☐
Can you produce a complete list of every AI agent operating in your environment — built, bought, embedded, and shadow?	☐	☐	☐
Does a governance record (agent card) exist for every agent with risk classification, approved scope, and evidence trail?	☐	☐	☐
Is there a formal pre-deployment gate every agent must pass before operating, with named sanctioning approval?	☐	☐	☐
Does your runtime governance validate agent behavior against sanctioned scope — not just monitor for threats?	☐	☐	☐
Can you demonstrate EU AI Act compliance on demand for any AI system, based on continuous evidence?	☐	☐	☐

Chapter 06 • Business Case

Building the Business Case

Most of the value of AI governance is risk reduction — invisible until the crisis arrives. Here is how to make the invisible visible for your executive team.



Make the invisible visible.

Most of the value of AI governance is risk reduction — invisible until the crisis arrives. Here is how to frame it for your executive team.

THE ACCOUNTABILITY QUESTION NOBODY IS ASKING LOUDLY ENOUGH

When an AI agent makes autonomous decisions affecting a customer, a transaction, or a medical workflow — **who is accountable? The organization that deployed the agent. Not the model provider. Not the platform vendor.** Satisfying that accountability requires a complete governance record: registry entry, agent card, constitution, pre-deployment approval, and runtime validation history.

Quantify the Risk (Cost of Doing Nothing)

EU AI Act regulatory penalty exposure
How to calculate: 7% × your global annual revenue = maximum fine per violation

Manual governance operational cost
How to calculate: 11–20 hrs/week × FTE cost × number of governance team members

Accountability gap: ungoverned autonomous agent actions
How to calculate: Number of agents × decisions/day × per-incident legal exposure

AI deployment delays due to governance bottlenecks
How to calculate: Number of AI projects × average delay × engineering and opportunity cost

Quantify the Return (Credo AI Value)

Governance intake time reduction OPERATIONAL	**Hours to Minutes with GAIA**
EU AI Act compliance acceleration COMPLIANCE	**10× faster documentation**
Risk review throughput OPERATIONAL	**60% faster with AI assistance**
Agent accountability record — on demand RISK	**Complete governance record for any agent at any time**
Audit response cost reduction COMPLIANCE	**Continuous audit-ready documentation**
AI deployment velocity STRATEGIC	**Governance as enabler, not bottleneck**

Typical Enterprise ROI Pattern (>1,000 AI use cases)

YEAR 1
Break-even or positive
Operational efficiency gains from GAIA + one avoided compliance incident

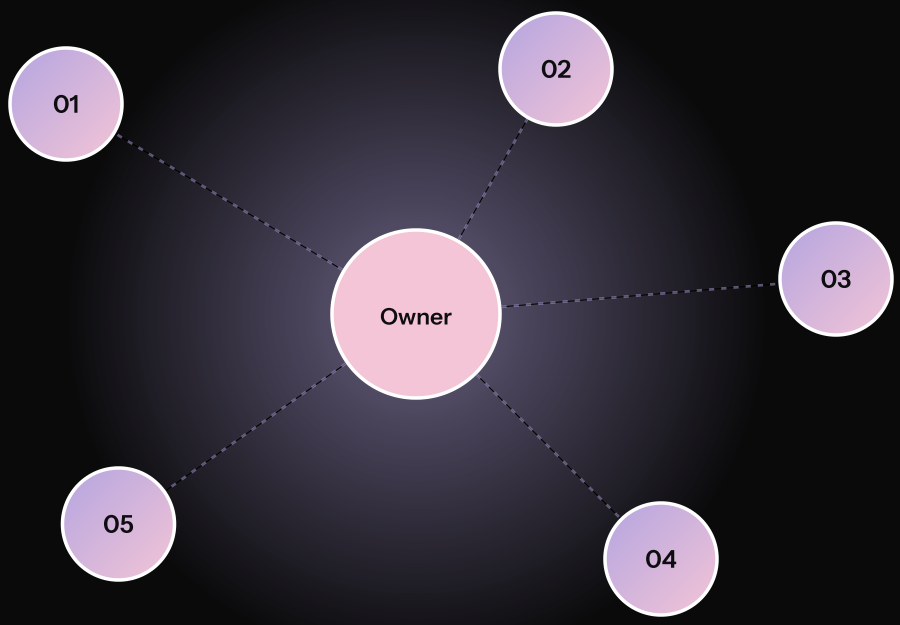
YEAR 2
3–5× ROI
EU AI Act readiness value + scaled governance across all AI systems

YEAR 3+
Compound returns
Governance-of-record switching costs compound — the accountability record cannot be built retroactively

Chapter 07 • Buying Committee

Navigating the Buying Committee

AI governance purchases span legal, risk, AI, security, data, and platform teams — each with different priorities and potential for veto. Map the committee before the first executive conversation.



Map your committee before the first conversation.

AI governance purchases span legal, risk, AI, security, data, and platform teams — each with different priorities and potential for veto.

WHO OWNS THIS?	WHO APPROVES?	WHO IS THE RISING BUYER?	WHO BENEFITS FIRST?	WHO MUST ALIGN?
Head of AI Governance / Chief AI Governance Officer / Chief Responsible AI Officer / CISO	**CDO / CAIO / CRO / General Counsel / CTO**	**CISO — increasingly the budget holder for AI governance**	**AI CoE / Responsible AI Leads / Governance Teams**	**Data / ML Platform / Legal / Compliance / Procurement**
Program credibility, regulatory defensibility, board confidence, AI risk posture	ROI, operational efficiency, regulatory risk, time-to-value	Per Forrester, security leaders now own AI risk end-to-end and are funding governance as part of the CISO mandate	Reduced manual burden, faster intake, consistent risk assessments, audit readiness	Integration with existing stack, no governance gaps between teams, shared accountability model

OWNERSHIP AMBIGUITY IS THE MOST COMMON REASON GOVERNANCE DEALS STALL OR FAIL POST-POC

Name one executive owner early

Someone whose performance review includes 'AI governance program.' Without a named owner, every team thinks another team is responsible.

Treat the CISO as a co-owner, not a gate

Forrester research confirms CISOs are no longer the blocker — they're the rising buyer for AI governance, owning AI risk end-to-end. Bring them in as a co-owner from day one: governance is the accountability layer above security, and the CISO is increasingly funding it.

Sequence legal and compliance together

Legal needs regulatory defensibility. Compliance needs audit trails. Both are served by the same governance record — brief them jointly, not sequentially.

What Drives Fast Time-to-Value

- ✓ **Pre-built regulatory content**
  EU AI Act, NIST, ISO policy packs — configured in weeks, not quarters.
- ✓ **AI-assisted configuration (GAIA)**
  Intelligent onboarding reduces manual setup burden.
- ✓ **Proven integrations with existing stack**
  MLOps, security, and observability — bidirectional.
- ✓ **Customer success governance expertise**
  Domain expertise, not just platform onboarding.

Red Flags in Any Evaluation

- × **12+ months to first use case**
  Not designed for enterprise adoption velocity.
- × **No pre-built regulatory content**
  Your legal team shouldn't build the vendor's policy pack.
- × **Platform vendor governing its own agents**
  Structural conflict: Microsoft cannot impartially govern Copilot.
- × **No AI assistance for governance workflows**
  Manual governance cannot scale with AI adoption.

Chapter 08 • About Credo AI

Measurable Trust. At Scale.

Credo AI is the AI governance platform of record for the Fortune 2000 — purpose-built to govern every AI system, model, agent, and application your enterprise deploys.

12
Perfect Forrester Wave™ Scores

30+
Enterprise Partners

2020
Pioneer in AI Governance

"The push to adopt AI is moving faster than the governance approach can keep pace with. Credo AI is the platform that closes that gap — not by slowing AI, but by governing it at the speed it moves."

Enterprise Customer · Fortune 500 Financial Services

RECOGNITION

Forrester Wave™ Leader
AI Governance Solutions · 12 Perfect Scores

#6 Fast Company
Most Innovative 2026, Applied AI

Gartner Cool Vendor
AI Governance

WEF Tech Pioneer
World Economic Forum

Ready to evaluate Credo AI?

We'll walk you through a live demo against your specific requirements — AI registry, EU AI Act, policy pack, Govern AI Assistant intake, and agentic governance.

Request a Demo | credo.ai →

WEBSITE
credo.ai

EMAIL
mktg@credo.ai

LINKEDIN
@credo-ai

ROI PLAYBOOK
Read the playbook →

STATE OF AI GOV
Read the report →