



AI GOVERNANCE

Eight questions to ask any AI-native vendor.

"Do you maintain an AI inventory?" is now the first question on every serious questionnaire you will receive. These are the eight that decide whether a vendor's agent belongs anywhere near your regulated data.

- 1 Which models, and who hosts them?**
Sub-processors, regions, and whether your data trains anything, now or later.

2 What can the agent do without a human?
Read, write, execute, spend. Where is that written down, and who approved it?

3 How do we stop it?
Kill switch, revocation, and who on our side can pull it, at 2 a.m.

4 What is logged, and can we get the log?
Every action attributable, exportable, retained for as long as our audit window.
- 5 What evaluations has it passed?**
Accuracy, bias, safety. Dated, repeatable, on data that looks like ours.

6 Does the BAA or DPA cover the AI feature?
Or does it predate it? A BAA that predates the vendor's new AI feature is a question to ask before the OCR does.

7 What is your incident and notification timeline?
For model failures, not just breaches.

8 Which framework are you certified against, and since when?
ISO 42001, SOC 2 with AI criteria, HITRUST AI, or none yet.

THE AI INVENTORY one row per system, yours and your vendors'

FIELD	WHAT TO CAPTURE	WHY IT MATTERS
System and provider	Name, vendor or internal team, business purpose	Accountability lands on a named executive under NIST AI RMF, ISO 42001 and the EU AI Act
Model and hosting	Model family, host, region, sub-processors, training use	A model swap is a material change to what you approved
Data touched	PHI, PII, PCI, CUI, internal only	Decides which agreements and controls apply
Risk class	EU AI Act tier, ISO 42001 impact, NIST AI RMF profile	Patient triage and claims coding are high-risk; a summarizer is not
Human oversight	Named owner, review cadence, escalation path	The first thing an auditor and a regulator ask
Evaluations and DPIA	Evals passed with dates; DPIA done or due	Proof the system was assessed before it touched real data
Autonomy policy	What it may do unattended, what needs a human, how you stop it	Without it, "can it spend money?" has no answer

IN KOLLGUARD

The eight questions are in the standard question bank

Every vendor on the register answers them. The AI inventory, classification and autonomy policy live in AI Governance; Agent Watch monitors the agents in production.

kollguard.com/for/enterprise

TALK TO US

Bring one vendor, we will run the bank

20 minutes on a live tenant. No slides.

raj@kollguard.com · 628-333-5116

ON STAGE IN 2026 Where KollGuard has pitched, exhibited and sponsored this year · kollguard.com/spotlight

- JUL 18–19**
AGI Summit
Startup track · customer exchange
- JUL 30 – AUG 1**
Stanford AI Summit
Exhibitor · main-stage pitch
- AUG 26–27**
Step SF
Spotlight Startup · pitch competition
- SEP 17–18**
ISACA Sacramento 2026
Platinum sponsor · speaker session