Shadow AI in the Supply Chain

Governing what you cannot see

Bram Ketting · Founder · 3rdRisk

Chlōe Dellow · Director, Office of the CISO, EMEA · Diligent

November 18, 2026

© 2024 Diligent Corporation

THE BIG IDEA

Shadow AI is more than an employee using an unapproved tool. It's AI entering your supply chain unseen.

It arrives through approved services, vendor operations, fourth parties and data flows - with no matching change in risk visibility. TPRM has to move from point-in-time assessment to continuous, proportionate governance.

WHERE IT ENTERS

Shadow AI is a supply-chain visibility problem

INSIDE THE ORGANISATION

Employees & teams

People using unapproved AI tools in their daily work.

INSIDE APPROVED VENDORS

New AI in old contracts

New AI features, copilots, model use and undisclosed changes - including AI used by subcontractors.

BEYOND THE VENDOR

The hidden chain

Model providers, cloud services, subprocessors and fourth parties.

The risk isn't policy-breaking — it's a missing inventory, data-flow view, control owner or change signal.

WHY IT MATTERS NOW

AI is already in operations - and on the breach ledger

88%

of organisations use AI in at least one business function, up from 78% a year earlier.

McKinsey, State of AI 2025

1 in 4

malicious breaches are AI-enabled — up 56%, costing $6M on average.

IBM, Cost of a Data Breach 2026

87%

name AI-related vulnerabilities their fastest-growing cyber risk.

WEF, Global Cybersecurity Outlook 2026

84%

of risk committees saw a third-party miss cause operational disruption.

Gartner (Feb 2023)

Don't ask *whether* a vendor uses AI. Ask where, how, and under what controls.

A SIMPLE TAXONOMY

Two categories of AI risk in the supply chain

ADOPTION-RELATED

What vendors do with AI

- Dependence on AI and model providers
- Quality, explainability and reliability of outputs
- AI outages hitting service availability
- Your data used to train or improve a model
- Unclear model-provider and subprocessor chains

VULNERABILITY-RELATED

What attackers do with AI

- AI-generated phishing and social engineering
- Deepfakes targeting vendor staff or executives
- AI-generated malware and automated exploitation
- Greater attack speed and scale

THE VENDOR BLIND SPOT

Due diligence tells you who a vendor was on the day you checked.

It doesn't tell you who they are today -or what they've quietly started running on the back end.

CHANGE 1

AI inside approved vendors

New features, data flows and model providers the last assessment never asked about.

CHANGE 2

Speed of change

Acquisitions, incidents, expired certifications and drift — all between review cycles.

CHANGE 3

Fourth parties & scale

Your vendor's vendor becomes your exposure, across more suppliers and jurisdictions.

MAKE IT ANSWERABLE

What to ask vendors about shadow AI

YOUR DATA

Where AI touches it

- Where and why is AI used in services affecting us?
- What customer data can enter the AI workflow?
- Is our data used to train or fine-tune a model?

THE CHAIN

Who's actually running it

- Which models, providers, clouds and subprocessors are involved?
- How are model and provider changes communicated to us?

RESILIENCE

What happens when it breaks

- How are output quality, bias and human oversight managed?
- How do you defend against AI phishing and deepfakes?
- How will you notify us of an AI-related incident?

THE NEW OPERATING MODEL

From annual reassessment to a continuous loop

01

Profile

A tailored risk profile: AI use, data flows, model providers, fourth parties.

→

02

Monitor

Continuously watch vendor changes, AI features, incidents and provider shifts.

→

03

Triage

Escalate meaningful change to the right owner; request targeted assurance.

→

04

Respond

Mitigate, change controls, use contract remedies — or exit.

↻ CONTINUOUS LOOP · NO ANNUAL ENDPOINT

Due diligence becomes the baseline. Continuous monitoring becomes the nervous system.

PROPORTIONALITY

Not every vendor needs the same depth

	LOW CRITICALITY	HIGH CRITICALITY
HIGH TRUST	**Baseline** AI disclosure, baseline contract terms, passive monitoring.	**Evidence** Detailed AI inventory, data-flow evidence, change notification, targeted assurance.
LOW TRUST	**Contain** Defined restrictions, limited data access, clear exit path.	**Start here** Intensive assurance, technical testing, executive ownership, contingency planning.

MAKE IT REAL

Signals, triggers and owners

SIGNALS

What changed

- New AI feature or changed model
- New provider, subprocessor or fourth party
- AI incident or security advisory
- Deepfake or impersonation of the vendor

TRIGGERS

What we do

- Re-profile the vendor
- Request targeted evidence
- Restrict data or feature use
- Escalate to the right owner

OWNERS

Who decides

- One accountable owner per trigger
- No generic TPRM queue for every signal
- Humans stay accountable for AI-assisted findings

A trigger without a named owner is just another alert.

YOUR STARTING PLAN

The first 90 days

DAYS 0–30

Discover

- Find critical vendors where AI could affect data, availability or decisions
- Build a first AI-use and fourth-party inventory
- Add shadow-AI questions to intake and renewal

DAYS 31–60

Prioritise

- Apply the trust-versus-criticality model
- Set minimum contract and change-notification terms
- Define first signals, triggers and owners

DAYS 61–90

Operate

- Continuously monitor a few critical vendors
- Run a tabletop: a vendor ships AI without notice
- Review one real signal end to end, then expand

WHAT TO REMEMBER

1. Shadow AI already enters through people, products, vendors and fourth parties — the risk is **unobserved change**.

2. Annual due diligence can't govern a continuously changing, AI-enabled supply chain.

3. Profile, monitor, triage, respond - proportionately, with a named owner for every decision.

Chlöe Dellow · Director, Office of the CISO, EMEA, Diligent
Bram Ketting · Founder, 3rdRisk

NEXT STEPS

Continue the journey…

THE WHITEPAPER

Continuous vendor risk management for the AI era

IDC InfoBrief, printed and at your seat. Scan to download the full report.

Scan to download

UPCOMING WEBINAR · 9 DEC 2026

The Vendor Blind Spot, Part 2: Who Owns Vendor AI Risk

IDC and Diligent continue the conversation. Scan to register.

Scan to register

Diligent