AI SECURITY ENGINEERING FIELD GUIDE · 2026

# Chapter 13 · Vendor Risk and AI Procurement

Standalone learning module for LMS delivery and required reading.

| FORMAT | USE | SCOPE | AUDIENCE |
| --- | --- | --- | --- |
| Standalone PDF | LMS reading module | Single chapter | Learners |

CHAPTER 13

# Vendor Risk and AI Procurement

**INSPECT**

AI features, model providers, connectors, training-use terms, retention, support access, and change controls.

**PRODUCE**

Vendor intake, connector review, contract notes, questionnaire evidence, and procurement recommendation.

> AI procurement is a security review of data, authority, evidence, and change.
>
> FIELD GUIDE

> **FIELD GUIDE: VENDOR REVIEW**
>
> Inspect AI features, model providers, connectors, training-use terms, retention, support access, evidence claims, and material-change controls.

This domain covers AI vendor risk, procurement, questionnaires, model provider terms, sub-processors, connector scopes, data retention, training on inputs, support access, trust-center claims, control evidence, and material-change monitoring. It matters when a vendor product processes sensitive data, embeds AI features, connects to enterprise systems, or makes claims buyers must rely on.

Procurement should treat AI features as changeable security surfaces. A vendor can add model calls, change a provider, expand a connector, alter retention, or publish a stronger claim after the first review. The review has to cover current use and material change.

> **FIELD USE**
>
> Review the vendor through four questions: what data enters, what authority the product receives, what evidence backs the claims, and what changes require notice or re-review.

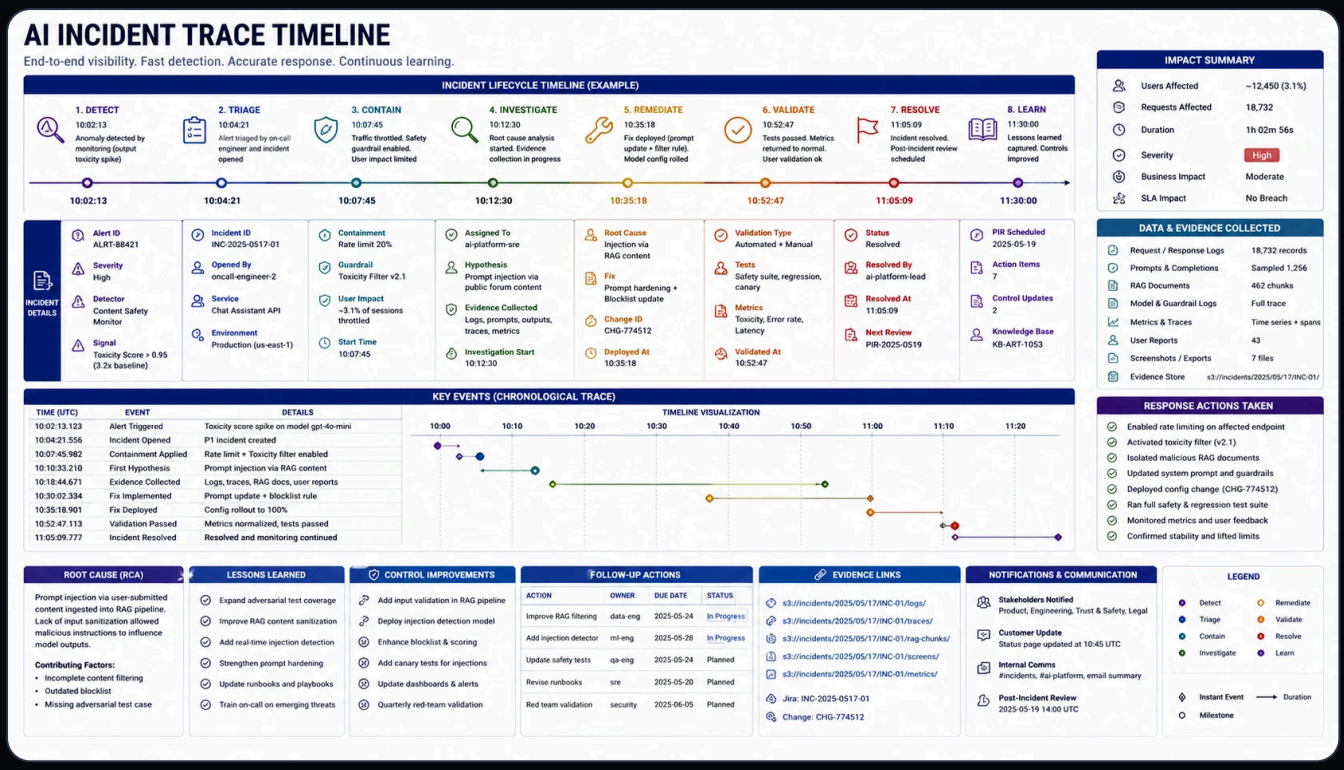


FIGURE 1: FIGURE 14: AI VENDOR PROCUREMENT MAP COVERING FEATURE INVENTORY, DATA FLOWS, CONNECTOR SCOPES, CLAIM-READINESS REVIEW, AND MATERIAL-CHANGE CONTROLS

## WHAT BREAKS HERE?

- Vendors describe AI features but not data flows or controls.
- Training-use, retention, support access, or sub-processor terms conflict with buyer requirements.
- Connectors request broad scopes without business justification.
- Trust-center claims are not tied to AI-specific evidence.
- Vendor AI features change without security re-review.
- Procurement accepts generic AI assurances that do not match the purchased configuration.

### WHAT TO INSPECT

- Vendor AI feature inventory and model/provider disclosure.
- Data processing terms, retention settings, training-use clauses, and regional processing.
- Connector scopes, admin permissions, support access, and audit logs.
- Security questionnaires, trust-center pages, SOC reports, AI policies, and eval claims.
- Contract language for material changes, incident notification, deletion, and evidence requests.
- Product settings that disable AI features, reduce retention, restrict training use, or limit connectors.

### WHAT TO ASK

- What AI features process customer data?
- Which model providers and sub-processors are involved?
- Is customer data used for training, fine-tuning, evals, or product improvement?
- What logs, prompts, outputs, embeddings, or files does the vendor retain?
- What connector permissions are required and why?
- How will the vendor notify buyers about AI feature changes?
- Which claims are evidence-backed for this product tier and configuration?

### WHAT TO TEST

- Compare questionnaire answers against trust-center and contract language.
- Review connector scopes against least privilege.
- Check admin controls for disabling AI features, retention, training use, and support access.
- Validate vendor incident notification and deletion commitments.
- Score public claims against evidence provided.
- Review AI material-change history.
- Compare requested connector scopes with the minimum workflow the business needs.

### CONTROLS AND GUARDRAILS

- AI vendor intake with feature, data, provider, connector, retention, and evidence fields.
- Contract clauses for training use, retention, deletion, sub-processors, support access, incidents, and material changes.
- Least-privilege connector review and periodic scope recertification.
- Claim-readiness review for vendor security and AI assertions.
- Procurement exception workflow with owner, expiry, and compensating controls.
- Material-change clause for AI features, providers, retention, sub-processors, and connectors.

### EVIDENCE TO COLLECT

- Vendor AI intake record.
- Data processing and retention notes.
- Connector permission review.
- Questionnaire answer pack.
- Trust-center evidence review.
- Contract risk notes.
- Procurement decision record.
- Material-change and connector-scope decision notes.

### OUTPUT ARTIFACTS

- Vendor/procurement checklist.
- AI vendor risk summary.
- Connector scope review.
- Questionnaire answer pack.
- Buyer evidence request list.

### RELATED SERVICES AND WORKBENCH TOOLS

| TYPE | RELATED PATHS |
| --- | --- |
| Workbench | Trust Scanner, AI Control Crosswalk, Surface Scanner |
| Services | Enterprise AI Security Readiness, AI Product Security Assessment, AI Security Operating Model |
| Handbook | Model and Provider Risk, Governance Evidence and Customer Trust, Data Exposure and Privacy |

### ARTIFACT: AI PROCUREMENT EVIDENCE PACK

Produce an AI vendor intake, connector review, contract notes, questionnaire evidence, and buyer-safe procurement recommendation.