

SAMPLE

AI Vendor Security Assessment Kit

The opening of vendor-evaluation-guide.docx, one of 8 files in the kit. <https://solasai.net/products/ai-vendor-assessment/>

AI Vendor Evaluation Guide

Solas AI | AI Vendor Security Assessment Kit solasai.net

How to run the assessment, interpret results, and monitor vendors over time.

When to Use This Kit

Run a full assessment when:

- Evaluating a new AI model provider for your product (OpenAI vs. Anthropic vs. self-hosted)
- Evaluating an AI SaaS tool for internal use (coding assistant, writing tool, analytics)
- An existing vendor makes material changes to their terms, pricing, or data handling
- Your annual vendor reassessment cycle triggers a review
- A vendor experiences a publicly disclosed security incident

Run a quick reassessment (Section Scores only, no full questionnaire) when:

- A vendor releases a new model version you plan to adopt
- A vendor updates their terms of service
- A vendor announces a sub-processor change
- Quarterly check-in on critical vendors

The Assessment Process

Step 1: Gather Information (1-2 hours per vendor)

Before sending the questionnaire to the vendor, collect what you can from public sources:

- **Trust/security page:** Most major providers have a trust center (e.g., trust.openai.com, anthropic.com/trust)
- **Terms of service and DPA:** Download and review. Use the DPA Requirements Checklist.
- **Compliance reports:** Request SOC 2 under NDA if not publicly available
- **Documentation:** API docs, data handling docs, privacy policy
- **Provider Quick Reference:** Check if the vendor is profiled in our Major Provider Quick Reference document — it gives you a head start

Pre-populate the questionnaire with what you can find. This reduces back-and-forth with the vendor.

Step 2: Complete the Questionnaire (30-60 minutes per vendor)

For information you cannot find publicly, send the relevant questions to the vendor's security or sales team. Most enterprise AI vendors have a security review process and will complete a questionnaire or provide equivalent documentation.

Score each answer using the 0-1-2 rubric. Be honest — a "1" (partial) is better than an inflated "2" that you cannot defend to your auditor or your customers.

Step 3: Complete the Comparison Matrix

If evaluating multiple vendors, transfer scores to the Comparison Matrix. The matrix gives you a side-by-side view that makes the decision visible to stakeholders who don't want to read 60-question questionnaires.

Step 4: Review DPA

Run the DPA Requirements Checklist against each vendor's data processing agreement. Flag any missing "Required" items — these need to be negotiated before you sign.

Step 5: Make the Decision

Use the weighted scoring in the Comparison Matrix final section. Present the recommendation with:

- Overall scores and ratings
- Critical item pass/fail status
- Cost comparison at your projected volume
- Key risks and compensating controls
- Recommended vendor with rationale

Step 6: Document and Archive

Keep the completed assessment, DPA checklist, and comparison matrix in your vendor management files. You will need them for:

- SOC 2 audits (auditors ask about vendor risk assessment)
- Customer security questionnaires (customers ask about your AI vendors)
- Annual reassessment baseline
- Incident response (if the vendor has a breach, you need to know what data they handle)

Scoring Guidance

What "2" Looks Like

The vendor fully meets the requirement with documented evidence. Examples:

- "Does the vendor hold SOC 2 Type II?" → Report available under NDA, current within 12 months
- "Does the DPA prohibit training?" → Explicit contractual clause, not just a blog post or FAQ

What "1" Looks Like

The vendor partially meets the requirement or meets it without documentation. Examples:

- "Does the vendor hold SOC 2 Type II?" → SOC 2 Type I (not Type II), or certification is in progress
- "Does the DPA prohibit training?" → API terms say no training, but DPA doesn't specifically address it

The sample ends here. The full document runs about 1,251 words; the kit holds 8 files. Version 2.2, 19 October 2026. Buy it at <https://solasai.net/products/ai-vendor-assessment/>, 14-day refund for any reason.