# AI service-provider oversight example

Qualified Individuals, financial-services security and procurement teams

[Read the complete guide on aona.ai](https://aona.ai)

For an institution covered by the FTC Safeguards Rule, an AI vendor receiving customer information belongs in the relevant service-provider review. Assess its ability to safeguard that information, require appropriate safeguards by contract and periodically reassess the provider. A product label does not establish those facts.

A fictional tax-preparation firm evaluates a limited wording task before permitting customer documents. Each finding leads to a specific evidence action.

Synthetic institution and procurement case. No real provider approval, contract or safeguards test is represented.

## Your review

Reviewer: ______________________ Date: ______________________

Organisation or team: ________________________________________

☐ **Confirm applicable coverage**

Identify the institution, customer-information categories and relevant provider role.

☐ **Match safeguards to the task**

Review capability evidence, contractual requirements and ongoing assessment as three separate checks.

☐ **Name the continuing owner**

Record who responds to service changes, incidents and periodic reassessment findings.

Checked items record your review, not a compliance approval or an installed-product test result.

### Notes and next actions

**Decision and scope:** _________________________________________________

**Evidence to collect:** _________________________________________________

**Owner and next review date:** _________________________________________________

## Review matrix

| Review area | Illustrative finding | Evidence action |
|---|---|---|
| Institution and information | Fictional covered tax-preparation firm; source files contain nonpublic client information. | Compliance owner confirms actual scope and data categories. |
| Necessity | Generic wording help does not require complete tax returns. | Business owner selects an invented or reduced-context first task. |

| Review area | Illustrative finding | Evidence action |
|---|---|---|
| Provider capability | Service-specific handling and safeguards have not been assessed in the scenario. | Security requests evidence relevant to the exact service and data flow. |
| Contract | Appropriate safeguards must be reflected in the applicable agreement. | Procurement records the actual obligations and unresolved terms. |
| Monitoring | No monitoring arrangement exists in the fictional starting proposal. | Assign a provider owner, review cadence and change triggers. |
| Test and decision | No live customer-data use or control test is authorised by the exercise. | Use synthetic material; record actual results and the accountable decision separately. |

## Three different evidence steps

- **Select:** Can the provider safeguard this information?
- **Contract:** What obligations apply to the actual service?
- **Reassess:** Are the safeguards still adequate as risk changes?

### Safe example task

“Improve the wording of a generic message telling a client how to arrange an appointment. Do not invent names, income, tax identifiers or account information.”

### Example disposition

Proceed only with the invented wording exercise. The customer-document proposal remains outside this teaching decision. Actual service terms, controls and accountable review must be established for any real customer-information use.

## Sources and scope

Sources checked 2026-09-21. Review the current requirements and your actual agreement before using this workbook for a real decision. General information, not professional approval or a completed control test. It is not the institution’s Qualified Individual or an automatic vendor-risk approval system. Its own handling requires review where relevant.

FTC: Safeguards Rule, what your business needs to know. Covered institutions, customer information, service-provider oversight and the notification threshold and process.

16 CFR 314.2: Definitions. Customer information, financial-institution scope and the definition and acquisition presumption for a notification event.

16 CFR 314.4: Information-security programme elements. Service-provider oversight under paragraph (f) and FTC notification timing, content and discovery under paragraph (j).