

Before anyone reads your AP data: the questions to ask

Finance AI security questions a controller or IT lead asks before anyone reads AP data, with the answers Rever publishes on its trust page.

Published 12 October 2026

Your accounts payable data holds vendor bank details, payment history, contract prices and the names of the people who approve spend. Before a recovery audit firm, a consultant or an AI vendor reads it, a controller and an IT lead work through a short set of finance AI security questions. You grant access on the strength of the answers.

Rever's agents read AP data to do their work, and Rever publishes its answers on [its security and trust page](#) and in its legal pages. Put the same questions to Rever as to anyone else, and ask for a document behind each answer.

Access: can the connection change anything?

Start with the connection. Ask whether the vendor needs read access or write access, which records it reads, and who holds the credentials. A party that can write to your ERP or your bank portal can post an entry or change a vendor's bank account, and each later answer has to cover that power.

Rever's connections to your ERP, banks and documents are read-only. The site describes each one as "a direct, deterministic integration rather than an MCP server or an agent holding credentials", so the agents can read what the connection provides and your source data stays unchanged.

Rever never writes to your systems. A journal entry your team approves comes back as an import file your team loads, a payment hold is recorded in Rever after Inbox approval and your team applies it in the payment run, and other corrections are prepared with their evidence for your team to action.

[Rever and the ERP you already run](#) covers the questions your ERP administrator will add.

Data use: what happens to the records once they leave

Your next questions concern the data itself: whether it trains a model, whose model, and what the vendor keeps when the engagement ends. AP records carry employee names and vendor bank accounts, so ask where personal data goes too.

Rever does not use customer data to train models. Its trust page says that what the agents learn about your business, from your policies, contracts and confirmed answers, stays within your tenancy. Rever handles personal data in connected records without human-readable exposure in model prompts, and does not store it in model context.

Rever keeps original records as received, before it transforms anything, and keeps calculations and source references connected to each finding and workpaper. Rever does not tie itself to a single model provider, and its model routing follows your hosting and data-residency requirements.

Finance AI security questions, with Rever's answers

Each row pairs a question with the document to request and Rever's published answer.

QUESTION	ASK TO SEE	REVER'S PUBLISHED ANSWER
Can it change our books or move money?	The connection's permission scope	Read-only connections; Rever never writes to your systems, and approved entries come back as an import file your team loads
Who holds the credentials?	The architecture	Direct, deterministic integrations, with no MCP server and no agent holding credentials
Does our data train a model?	The data-processing terms	No training on customer data
Where does personal data go?	The DPA and the sub-processor list	No human-readable PII in model context
Are we separated from other customers?	The architecture	Tenant isolation at every layer, with guardrails around each agent
Where does it run?	The deployment options in the Order Form	Self-host, private cloud or managed cloud
Is the data encrypted?	The security measures	Encrypted at rest and in transit; rever.ai/legal/security-measures names AES-256 and TLS 1.2 or higher
What independent assurance exists?	The audit report and certificate	SOC 2 Type II, audited each year; ISO/IEC 27001:2022, certified
Who can log in?	The access model	SSO, SAML and SCIM for enterprise access control

Location: where the data lives

Your IT lead will want to know who operates the infrastructure, which region holds the data, and whether the platform can sit inside your own perimeter.

Rever offers three options with the same read-only rules. Self-host runs the full platform inside your own environment. Private cloud is a single-tenant deployment, dedicated and region-pinned, with model routing and processing locations specified in your Order Form. Managed cloud is Rever's own cloud, tenant-isolated and region-pinned, with Rever operating the platform. Rever's pricing places self-hosting and private cloud on the Enterprise plan.

People and decisions: who sees what, and who approves

A vendor's answer on access has two halves: which of its staff can see your data, and how your own team controls logins and approvals.

Your administrators control your users and roles in Rever, including preparer, approver and auditor roles. SSO, SAML and SCIM are available for enterprise access control.

You set approval thresholds and dual approval for material amounts. Rever's floors apply in every plan, including Free: nothing leaves Rever without a recorded approval from an authorised approver, and the identity that prepares an action cannot approve it. Rever records each approval, question and send-back as a decision in the Inbox, with what happened next. Sentinel flags suspicious vendor-bank changes and payment patterns, Auditor tests procedures on its own cycle, and Steward checks system health. The site sums up the split in one line: "Agents prepare. Your team approves."

The paperwork to request

Request the documents before the first connection, so your IT review runs in parallel with the business conversation. Rever makes its security pack available on request: the SOC 2 Type II report, the ISO/IEC 27001:2022 certificate, the architecture and the data-processing terms. Its security measures page says Rever shares reports and certificates under a non-disclosure agreement.

Three legal pages answer the contract questions in public: the [data processing agreement](#), the [list of sub-processors](#) and the [security measures](#).

Once your team accepts the answers, [the zero-day scan](#) runs on the same read-only connections, on a scope you agree: which entity, which systems, which period.

Questions

Is our financial data used to train AI models?

No. Rever does not use customer data for training, and what the agents learn about your business from your policies, contracts and confirmed answers stays within your tenancy.

What finance AI security questions should we ask a vendor?

Ask what the connection can read and change, whether your data trains a model, where the platform runs, who can log in, and which audit report and certificate back the answers. Rever answers each on its trust page: read-only connections, no training on customer data, self-host, private cloud or managed cloud, SSO, SAML and SCIM, and SOC 2 Type II and ISO/IEC 27001:2022.

Can we see Rever's SOC 2 report?

Yes. Rever makes the SOC 2 Type II report, the ISO/IEC 27001:2022 certificate, the architecture and the data-processing terms available on request, and shares reports and certificates under a non-disclosure agreement.

