

Questions to ask any vendor proposing a self-hosted integration

When agencies are asked to host custom third-party integrations, the security of that code often becomes the agency's problem. Use these questions in RFPs, contract renewals and security reviews to find out who owns the risk before you sign.

Use it in procurement. Add these questions to RFP security sections and vendor questionnaires.

Get answers in writing. Ask for evidence (reports, policies, contract language), not verbal assurances.

Apply it to every integration. Payments, GIS, document management, plan review, ERP and more.

1 Code ownership & continuity

If you can't name who owns and maintains the code, nobody does.

- ☐ Who owns the integration source code? Will we receive it, or will it be held in escrow with clear release triggers?
- ☐ Is this a standard, versioned product shared across customers, or one-off custom code written only for us?
- ☐ If the developer leaves, or your company is acquired or exits the market, who supports the integration?
- ☐ Is the code documented well enough that our staff or another vendor could maintain it?

2 Maintenance & lifecycle

Integrations break when either system changes, and vulnerabilities keep surfacing after go-live.

- ☐ Who patches the integration *and* everything under it: runtime, libraries, operating system, database?
- ☐ What is your committed timeline to fix critical and known-exploited vulnerabilities? (CISA and the FBI call for no more than 30 days.¹)
- ☐ How long is the support period, and how will we be told about end-of-support?¹
- ☐ When our core system or a connected system updates its API, who updates, tests and redeploys the integration, and at whose cost?
- ☐ Who monitors the integration for failures and security events, during what hours, and how are we alerted?

3 Software supply chain & secure development

Most integration code is built on open-source components you can't see, so how it's built matters.

- ☐ Do you follow a recognized secure development framework, such as NIST SP 800-218 (SSDF) or OWASP SAMM, and will you attest to it?²
- ☐ Is the code peer-reviewed and scanned (static, dependency and secrets scanning) before every release?

4 Independent audit & assurance

A vendor's SOC 2 report often covers the core product, not the custom code on your server.

- ☐ Is the integration explicitly in scope of your SOC 2 Type II, ISO 27001 or GovRAMP (formerly StateRAMP) assessment?³
- ☐ Will you support our own security audits and assessments, and fix findings at your cost and within a set timeframe?

5 Total cost of ownership & exit

- ☐ What servers, OS and database licenses, backups and agency staff time does hosting require each year?
- ☐ What does it cost to upgrade, re-test or rebuild the integration when systems change?
- ☐ If we move to a different approach, what is the exit plan for code, data, documentation and handoff?

6 Access, credentials & data protection

Integrations hold the keys to multiple systems at once.

- ☐ Where are passwords, API keys and service-account secrets stored? Are any hard-coded or in plain-text config files?¹
- ☐ What network access does the integration need: inbound firewall ports, domain accounts, admin rights? Is it least-privilege?
- ☐ Does your staff need remote access (VPN, RDP, remote desktop tools) to our servers? Is it MFA-protected, time-limited and logged?¹
- ☐ Is data encrypted in transit and at rest, including temp files, queues, logs and backups?
- ☐ What activity is logged, in what format, and for how long? (CISA and the FBI recommend at least six months.¹)

7 Compliance, incident response & liability

Self-hosting can shift regulatory scope and breach liability onto the agency.

- ☐ Which of our obligations does the integration touch: PCI DSS (payments), CJIS, HIPAA, state privacy and breach-notification laws, records retention?
- ☐ If it handles card data, does it fall within our PCI scope and our required inventory of custom software (PCI DSS Req. 6.3.2)?⁴
- ☐ If the integration is the entry point for an incident, who leads response and notification, and how fast will you engage?
- ☐ What cyber liability insurance do you carry, and does the contract indemnify us for incidents caused by your code?

Red flags to listen for

- ⚠️ “Once it’s installed, your IT team owns it.”
- ⚠️ “Our SOC 2 covers the platform” (but not the integration).
- ⚠️ “API changes are billed as new work.”
- ⚠️ “We’ll need a VPN account to support it.”
- ⚠️ “The credentials are in the config file.”
- ⚠️ No written patch timelines or support end date.

What strong answers look like

Clear accountability

The vendor owns patching, monitoring and API updates, with written timelines.

Minimal footprint

No standing remote access or inbound ports; secrets kept in a managed vault, not files.

In audit scope

The integration itself is covered by SOC 2, ISO 27001 or GovRAMP reports.

Compliance mapped

PCI, CJIS and privacy obligations are documented, with defined incident roles.

Secure development

A recognized secure development framework, with code review and scanning before every release.

Clean exit

Code, data and documentation handoff are written into the contract.

Sources. [1] CISA & FBI, *Product Security Bad Practices* v2, Jan. 2025 (cisa.gov). [2] NIST SP 800-218, *Secure Software Development Framework*, 2022; OWASP, *Software Assurance Maturity Model (SAMM)* v2 (owasp-samm.org). [3] GovRAMP (formerly StateRAMP), rebranded 2025. [4] PCI Security Standards Council, *PCI DSS v4.0.1*, Req. 6.3.2, mandatory since Mar. 31, 2025. See also CISA, *Principles and Approaches for Secure by Design Software*, Oct. 2023.