



SOC 2 compliance software evaluation checklist

A companion to our guide on the best SOC 2 compliance software. Use it to pressure-test a vendor's answers against six criteria that actually separate a strong platform from a well-marketed one.

Each item includes a red flag to listen for during a demo or sales call. Tick a box only once you've seen the control, not once someone has described it.



Automation

- ☐ Evidence collection covers every system in your stack, not just the most common integrations
Red flag: Automation only covers “popular” integrations, everything else needs manual upload.
- ☐ Control monitoring runs continuously, not on a scheduled check-in
Red flag: “Continuous monitoring” turns out to mean a weekly or monthly sync.
- ☐ Employee onboarding and offboarding changes flow into the platform automatically
Red flag: Access changes still require someone to manually update a ticket or spreadsheet.

Audit readiness tools

- ☐ The audit dashboard is something you can see live, not just described in a sales call
Red flag: The vendor won't provide a working demo of the actual dashboard.
- ☐ Auditors get their own access portal, separate from your internal team's login
Red flag: Auditor access means someone on your team manually exporting and emailing documents.
- ☐ The platform supports real-time interaction with controls, if your audit firm expects that
Red flag: Every auditor question requires a new export or screenshot.

Integrations

- ☐ Every system in your actual stack is listed as supported: cloud providers, HR tools, ticketing, identity providers
Red flag: “Integration” turns out to mean a generic CSV import, not a live connection.

- ☐ There's a clear process and timeline for systems without a native integration
Red flag: No answer beyond "we can build a custom one," with no timeline or cost attached.
- ☐ Integration setup time is disclosed upfront, not discovered during onboarding
Red flag: Setup estimates change significantly once the contract is signed.

Vendor risk management

- ☐ Risk questionnaires are customizable to your actual vendor list, not a fixed generic template
Red flag: One questionnaire is used for every vendor regardless of what data they touch.
- ☐ Vendor monitoring continues after onboarding, not just a one-time assessment
Red flag: Vendor risk scores are set once and never revisited.
- ☐ Vendor risk data feeds into your overall compliance posture, not a separate siloed report
Red flag: Vendor risk lives in a disconnected spreadsheet outside the main platform.

Multi-framework support

- ☐ Frameworks you'll need next (ISO 27001, HIPAA, GDPR) are supported today, not listed as "coming soon"
Red flag: Sales says multi-framework support is on the roadmap for later this year.
- ☐ Overlapping controls across frameworks are mapped automatically
Red flag: Each framework requires a completely separate setup process from scratch.

- ☐ Adding a new framework later doesn't require re-collecting evidence you already have

Red flag: Every new framework means starting evidence collection over.

Security testing capabilities

- ☐ The platform distinguishes between documenting a control and validating that it works

Red flag: "Security testing" turns out to mean a checklist question, not an actual test.

- ☐ There's a clear path to pairing the platform with a penetration testing tool if testing isn't built in

Red flag: No guidance at all on how technical controls get validated beyond documentation.

- ☐ Test results map back to specific SOC 2 controls, not a generic vulnerability list

Red flag: Findings have no connection to which control they support or undermine.

Validate controls, not just documentation

Beagle Security runs agentic penetration tests mapped to SOC 2's security criteria, with OWASP-mapped reports and authenticated testing built in. Pair it with your compliance platform to back up documentation with real evidence. Start a 14-day free trial with Advanced plan features, no credit card required, or take the interactive demo for a self-guided look first.