



Free guide · SOC 2 · 2026

SOC 2 automation tool buyer's guide (2026)

What a SOC 2 automation platform can and cannot do for you, how to scope it against the AICPA Trust Services Criteria, the auditor-independence red flags the AICPA itself flagged in 2026, and a side-by-side of 13 tools from our verified dataset.

Last reviewed 16 Oct 2026 13 tools compared 8 sources

Independent and unsponsored. No vendor paid to appear in this guide. Pricing and features are as published by vendors at our last check (dates shown) and can change, so confirm with each vendor. This is not audit or legal advice.

SOC 2 in one minute

A SOC 2 examination reports on controls at a service organisation relevant to security, availability, processing integrity, confidentiality or privacy [\[1\]](#). It is performed by a CPA under the AICPA attestation standards and results in an opinion, not a certificate [\[6\]](#). A **type 1** report covers the system description and whether controls were suitably designed as of a date. A **type 2** report also covers whether those controls operated effectively throughout a period [\[7\]](#).

Automation platforms help you *prepare for* and *stay ready for* the examination. They connect to your systems, collect evidence, monitor controls, manage policies and often answer security questionnaires. Many now market AI agents for these tasks. The examination itself is still done by an independent CPA firm.

The Trust Services Criteria you are buying against

SOC 2 uses the AICPA's *2017 Trust Services Criteria (With Revised Points of Focus – 2022)*. The criteria follow the 17 COSO 2013 principles (CC1–CC5: control environment, information and communication, risk assessment, monitoring, control activities). Supplemental common criteria cover logical and physical access (CC6), system operations (CC7), change management (CC8) and risk mitigation, including vendors and business partners (CC9). The 2022 revisions changed only the points of focus, not the criteria [\[2\]](#).

Category	Criteria used
Security	Common criteria only (CC1–CC9). The common criteria apply to every category, so they are part of every SOC 2 examination.
Availability	Common criteria plus the A series.

Category	Criteria used
Processing integrity	Common criteria plus the PI series.
Confidentiality	Common criteria plus the C series.
Privacy	Common criteria plus the P series.

Source: AICPA TSP section 100 ¶1.08–10 [\[2\]](#).

The tool is not the auditor: 2026 red flags from the AICPA

In 2026 the AICPA published several warnings about "fast and easy" SOC 2 offerings tied to software platforms. If a vendor bundles the audit, check the points below.

- ☐ A SOC 2 report is an attestation examination performed by a licensed CPA under the AICPA attestation standards (SSAEs). It is not a certification, and a software tool cannot issue one. [\[6\]](#)
- ☐ Choose your CPA firm yourself, or at least confirm you can. The AICPA ethics staff warn that "bundled services", where the tool provider sells a package that includes the SOC 2 examination and sets the examination fee, can impair the auditor's independence. The examination fee must be set by the service auditor. [\[4\]](#)
- ☐ Treat promises of a guaranteed "clean audit" or a "100% pass rate", or claims that an auditor is "AICPA-approved", as red flags. The AICPA cites these as examples of advertising the Code may prohibit. [\[4\]](#)
- ☐ Be wary of fixed, tool-driven deadlines. Arrangements that limit the auditor's ability to set scope and timing, obtain evidence or communicate deficiencies create ethics and independence threats. [\[4\]](#)
- ☐ Ask the auditor to describe its risk assessment and testing for your environment. AICPA peer review now looks for SOC 2 engagements with identical reports, risk assessments, sample sizes and testing procedures across clients, which it treats as "nonconforming". [\[5\]](#)

- ☐ Verify the signing firm is licensed and enrolled in peer review. The AICPA has said it is looking into anonymously published allegations about a compliance vendor offering SOC services, and that unlicensed signatories may be referred to state boards of accountancy.
[\[3\]](#)

Evaluation checklist

- ☐ Scope first: decide which trust services categories your customers actually ask for. Security (the common criteria) is always included; add Availability, Processing Integrity, Confidentiality or Privacy only if you make commitments in those areas.

AICPA TSC ¶1.09–.10 · [\[2\]](#)

- ☐ Decide type 1 or type 2. A type 1 covers the system description and the suitability of control design as of a date. A type 2 also covers whether controls operated effectively throughout a period. Ask the tool vendor how its evidence collection supports a full type 2 period, not just a point-in-time snapshot.

AICPA SOC 2 Guide · [\[7\]](#)

- ☐ Map integrations to your stack: identity provider, cloud accounts, code repositories, HRIS, MDM/endpoint and ticketing. Evidence a tool cannot collect automatically becomes manual work.

Buyer practice

- ☐ Check how controls map to the criteria (CC1–CC9 and any category series) and whether you can edit, add or remove controls. The AICPA says points of focus may not all be relevant and management can tailor them.

AICPA TSC ¶1.05–.07 · [\[2\]](#)

- ☐ If you need several frameworks (ISO 27001, HIPAA, DPDP), check cross-mapping so one control satisfies several frameworks. Our listings show verified framework tags and vendor-claimed frameworks separately.

Agent Index dataset · [\[8\]](#)

- ☐ For AI agent features: ask which actions an agent can take without a human (for example, closing a finding or changing a policy), whether every agent action is logged, and whether you can export those logs to your auditor.

Buyer practice

- ☐ Ask whether customer data, evidence or policies are used to train models, and where evidence is stored (region, sub-processors).

Buyer practice

- ☐ Confirm the total cost: platform fee, per-framework modules, trust center, questionnaire automation, penetration testing and the audit itself. Several vendors list pricing only on AWS Marketplace or by quote.
- Agent Index dataset · [\[8\]](#)

SOC 2 automation tools compared

All 13 listings in the Agent Index [compliance](#) category tagged for SOC 2, in alphabetical order. "Frameworks" shows our verified tags. "Vendor-claimed" lists frameworks the vendor markets, which we have not verified individually. Each name links to the full profile with its sources.

Tool	What it does	Agent / automation tasks	Frameworks (verified · vendor-claimed)	Last verified
Comp AI Comp AI	Open-source-leaning AI compliance software that automates evidence collection, policy generation, and continuous monitoring for SOC 2, ISO 27001, HIPAA and GDPR.	evidence collection, policy management, control monitoring, trust center	SOC 2, ISO 27001, HIPAA · GDPR, FedRAMP	15 Oct 2026
Drata Drata	Compliance and trust management platform with AI-assisted evidence collection, continuous control monitoring, and multi-framework programs.	evidence collection, control monitoring, questionnaire automation, vendor risk, trust center	SOC 2, ISO 27001, HIPAA · GDPR, PCI DSS, NIST	16 Oct 2026
Hyperproof Hyperproof	AI-powered GRC platform for program management, evidence, audits and multi-framework compliance.	evidence collection, audit management, control mapping	SOC 2, ISO 27001, HIPAA · NIST, PCI	15 Oct 2026
Optro (formerly AuditBoard) Optro, Inc. (formerly AuditBoard)	AI-powered GRC Intelligence Platform (formerly AuditBoard) with domain-trained agents for audit testing, compliance, third-party risk and AI governance.	grc intelligence, risk management, control testing, audit management, vendor risk, ai governance	SOC 2, ISO 27001 · SOX, NIST	16 Oct 2026
Rippling Automated Compliance Rippling	Compliance automation built into Rippling's HR and IT platform, with AI framework setup, evidence collection, in-platform AI remediation, an audit portal and Trust Centers.	evidence collection, control monitoring, remediation, audit management, trust center, questionnaire automation	SOC 2, ISO 27001, HIPAA	16 Oct 2026
Scrut Automation Scrut Automation	Compliance and risk automation platform popular with startups and mid-market teams for continuous control monitoring and multi-framework programs.	evidence collection, control monitoring, questionnaire automation, risk management	SOC 2, ISO 27001, HIPAA · GDPR, PCI DSS	15 Oct 2026

Tool	What it does	Agent / automation tasks	Frameworks (verified · vendor-claimed)	Last verified
Scytale Scytale	AI-powered security and compliance platform combining agentic GRC automation with optional in-house GRC expert consulting bundles.	evidence collection, gap analysis, questionnaire automation, vendor risk, pen test management	SOC 2, ISO 27001, HIPAA · GDPR, SOX ITGC, ISO 42001	15 Oct 2026
Secureframe Secureframe	Compliance automation platform with Comply AI features for policies, remediation, risk, questionnaires and TPRM, plus Trust Center and CMMC/Defense packages.	evidence collection, policy management, questionnaire automation, vendor risk, trust center	SOC 2, ISO 27001, HIPAA · PCI DSS, CMMC	15 Oct 2026
Sprinto Sprinto	Autonomous compliance platform aimed at SaaS and growth-stage teams, with AI agents for mapping obligations, gathering evidence, and monitoring controls.	evidence collection, control monitoring, policy management	SOC 2, ISO 27001, HIPAA · GDPR, PCI DSS, ISO 42001	15 Oct 2026
Strike Graph Strike Graph	Compliance platform with published product pricing pages for building and maintaining security certification programs.	evidence collection, control mapping	SOC 2, ISO 27001, HIPAA · GDPR	15 Oct 2026
Thoropass Thoropass	Compliance platform that combines software with audit delivery pathways for SOC 2 and related frameworks.	evidence collection, audit management	SOC 2, ISO 27001, HIPAA · GDPR	15 Oct 2026
Vanta Vanta Inc.	Agentic trust and compliance automation platform for continuous evidence collection, control monitoring, policies, and security questionnaire responses.	evidence collection, control monitoring, questionnaire automation, policy management, trust center	SOC 2, ISO 27001, HIPAA · PCI DSS, GDPR, CMMC, NIST, FedRAMP	15 Oct 2026
Zania Zania Inc.	Agentic AI platform for enterprise GRC that executes third-party risk, controls testing, evidence collection, questionnaires and gap analyses with explainability.	vendor risk, controls testing, evidence collection, questionnaire automation, gap analysis	SOC 2, ISO 27001, HIPAA · GDPR, PCI DSS, ISO 42001, NIST CSF	15 Oct 2026

Source: Agent Index dataset [\[8\]](#). Related tools outside this table: [LogicGate Risk Cloud](#), [Conveyor](#), [SafeBase](#) (GRC, trust center and questionnaire automation).

Published pricing

Most SOC 2 platforms quote prices individually. Where a public figure exists, this is what we recorded. Figures from AWS Marketplace or third-party sources are labelled as such.

Tool	Pricing as recorded
Comp AI	Quote-based (Startup / Mid-Market / Enterprise). Specific dollar amounts not published on the homepage at last check.
Drata	Quote-based. AWS Marketplace Foundation Package listed at \$15,000/year for 1–50 employees (third-party census of marketplace listing).
Hyperproof	No public pricing verified at last check.
Optro (formerly AuditBoard)	No public pricing verified at last check.
Rippling Automated Compliance	No public pricing verified at last check.
Scrut Automation	Public pricing page not available (404 at last check). Industry AWS Marketplace census has listed \$15,000/year for up to 20 employees — treat as secondary pending vendor confirmation.
Scytale	Quote-based packages (Build Starter, Build DFY, Build Stronger; Scale; Enterprise). Dollar amounts not published on the public pricing page.
Secureframe	Quote-based. Public page lists Fundamentals / Complete / Defense feature packages without dollar amounts on the pricing page at last check.
Sprinto	AWS Marketplace: Starter Platform \$7,500/year (up to 100 employees) plus first compliance framework from \$2,000/year (combined entry often cited as \$9,500/year).
Strike Graph	Published on vendor pricing page (see source); verify current tiers on strikegraph.com/pricing .
Thoropass	No public pricing verified at last check.
Vanta	Quote-based. AWS Marketplace lists Essentials from \$14,000/year for 1–20 employees (12-month contracts); modules priced separately.
Zania	No public pricing verified at last check.

4 of 13 tools have a dollar figure on a public page we could verify. Audit fees are separate from platform fees unless a vendor states otherwise. Source: Agent Index dataset [\[8\]](#).

Next steps

Sources

1. AICPA & CIMA, "SOC 2® – SOC for Service Organizations: Trust Services Criteria". <https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2>

2. AICPA, "2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)" (TSP section 100). <https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022>
3. AICPA & CIMA, "System and Organization Controls: SOC Suite of Services" (includes the AICPA notice on SOC service vendors). <https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services>
4. AICPA Professional Ethics Division staff, "SOC engagements: Ethics risks with tool providers", Journal of Accountancy, 6 Apr 2026. <https://www.journalofaccountancy.com/issues/2026/apr/soc-engagements-ethics-risks-with-tool-providers/>
5. T. Kindem (AICPA), "AICPA guides peer reviewers to address SOC 2 risks", Journal of Accountancy, 14 May 2026. <https://www.journalofaccountancy.com/issues/2026/may/aicpa-guides-peer-reviewers-to-address-soc-2-risks/>
6. Journal of Accountancy podcast, "The risks of quick-turn SOC engagements and what CPAs should know", 30 Apr 2026. <https://www.journalofaccountancy.com/podcast/2026/apr/the-risks-of-quick%E2%80%91turn-soc-engagements-and-what-cpas-should-know/>
7. AICPA SOC 2® Guide text on type 1 and type 2 examinations (as published in PwC Viewpoint, AICPA guide library). https://viewpoint.pwc.com/dt/us/en/aicpav2/aag-sop/aag-sop/aag-sop3/aag-sop3_obtaining_written_representations.html
8. Agent Index dataset v0.1.1 (agents.json), each listing links its own vendor sources. <https://agentindex.heritageservices.online/agents.json>

Prepared by Agent Index (Heritage Services). Last reviewed 16 Oct 2026. SOC 2® is a registered trademark of the AICPA. Vendors: to correct a fact, use [Submit / Claim](#). Licensed CC BY 4.0.