SOC 2 TYPE II FOR STARTUPS · DATASHEET

Safeguard

Win the security review without hiring a compliance team.

A flat public price for companies under 10 people, with software and evidence in one place and the audit arranged separately.

THE PROBLEM

An enterprise customer asks for your SOC 2 report before it will sign, and you have no compliance team. The work is spread across spreadsheets, screenshots and a dozen systems, and the auditor starts from a pile of evidence you gathered by hand. The deal waits while you work out where to begin.

WHAT IT DOES

Start from the framework

Switch on SOC 2 and see its controls, policy templates and a readiness score, so you know what is left before the audit starts.

Evidence collects itself

Connect cloud accounts, identity providers and code hosts. Automated tests run against your systems and attach evidence to the controls.

Policies and questionnaires

Start from policy templates, keep a risk and vendor register, and answer customer security questionnaires from the same record.

Audit arranged separately

The audit is arranged through an accredited auditor network and billed separately. Audit fees are not part of the subscription.

HOW IT WORKS

1. **Choose** — Switch on SOC 2 for your workspace
2. **Connect** — Cloud, identity and code systems
3. **Test** — Automated tests collect evidence
4. **Close gaps** — Policies, risks, vendors and attestations
5. **Audit** — Accredited auditor network, billed separately

THE PRICE, PLAINLY

USD 1,699 a year for companies under 10 people; audit fees separate. The same subscription also covers your application and supply-chain security. Above ten people, standard pricing applies.

CAPABILITIES IN DETAIL

Price	USD 1,699 a year for companies under 10 people; audit fees separate. Current plans are at safeguard.sh/pricing.
Framework	SOC 2 Type II, with its scan requirements, controls and policy templates.
Evidence	Automated tests through connected systems such as Google Workspace, Google Cloud, GitLab and Jira, plus uploaded evidence and attestations.
Readiness score	The share of in-scope requirements that pass. It is Safeguard's assessment of what it can see, not an audit opinion.
Policies	Templates to start from, including access control, incident response and vendor risk.
Questionnaires and vendors	Answer inbound security questionnaires, keep a risk register and manage vendors.
Trust Center	Publish your security posture to customers and control who can see your documents.
Beyond compliance	The same subscription covers application and supply-chain security.

INPUTS

- Cloud accounts and identity providers
- Code hosts
- Your existing policies, if any
- Evidence a scan cannot see, attested by a person

OUTPUTS

- Readiness score and control status
- Collected evidence
- Policy drafts
- Answers to customer questionnaires
- A Trust Center page

INTEGRATIONS AND SURFACES

Google Workspace · Google Cloud · GitLab · Jira · Cloudflare · Trust Center · Questionnaires · Policy templates

DEPLOYMENT AND DATA HANDLING

Audit
Arranged through an accredited auditor network, billed separately from the subscription.

Regions and hosting
SaaS in US, EU (Frankfurt) and Gov regions. Private VPC, on-prem and fully air-gapped deployments are available.

Tenant isolation
Evidence and findings are scoped to your tenant and organization.

Access control
SSO (SAML 2.0, OpenID, Google, Microsoft, GitHub), roles and 2FA.

Safeguard helps you produce evidence and map controls. It does not make an organization compliant by itself.

Start with SOC 2

safeguard.sh/solutions/startups

Scan the code or type the address. Questions: hi@safeguard.sh

Safeguard

SOC 2 Type I and Type II audited; reports available on request (safeguard.sh/trust). Designed for FedRAMP High.