Srasta — SOC 2 Roadmap & Public Commitment

Version: 1.0 · **Last updated:** 2026-04-29 · **Status:** Pre-seed paper-stage; engineering work begins post-seed-close.

Public commitment (the paragraph)

> **Srasta is committed to SOC 2 Type I attestation by Q1 2027 and SOC 2 Type II attestation by Q4 2027.** Drata is our compliance automation vendor; auditor selection from Drata's partner network is finalized within two weeks of seed-close. The Type I audit period runs Q4 2026, with the Type I report issued in Q1 2027. The Type II observation period runs from Q1 2027 through Q3 2027, with the Type II report issued by end of Q4 2027. Until then, our SOC 2 Common Criteria controls matrix (`docs/security/controls-matrix.md`) and architectural data-flow diagram (`docs/security/architecture.md`) are the operative evidence artifacts for buyer security review.

This paragraph is the canonical public statement. When in doubt about wording in the website footer, pitch deck, or investor data room, copy from here.

Why a dated commitment

Regulated-adjacent buyers and tier-1/2 VCs ask the same question in the first call: *when will you have SOC 2?* An undated answer ("we're working on it") gets discounted; a dated answer with a named vendor and a budgeted plan gets credit. This document is the dated answer.

The dates are realistic given:

- Solo-founder pre-seed engineering effort (no compliance staff).
- Drata's typical 8-12 week onboarding-to-Type-I cadence for startups using their partner-auditor network.
- Type II requiring 6-12 months of continuous control operation before the report can be issued.

If seed close slips by ≥ 60 days, every milestone below shifts by the same amount — this is the rule, not an exception.

Timeline (anchored to seed-close = T0)

Phase	Window	Output
Pre-seed (today through T0)	Now → seed-close	Paper artifacts: controls matrix (#156, ✅), architecture + PDF (#157, ✅), privacy policy + CAIQ Lite (#158, ✅), this roadmap (#159, ✅), pitch deck v1 (#160, in flight).
Phase 1.1 — Vendor onboarding	T0 + 2 weeks	Drata account, integrations connected (GitLab, AWS, Google Workspace, 1Password, Linear), Type I scope frozen. DPA template authored by outside counsel concurrently (1 week).
Phase 1.2 — Controls implementation sprint	T0 + 2 weeks → T0 + 8 weeks	Drata-generated gap list resolved. Identity hardening (MFA on all admin), formal access reviews, asset inventory, vendor risk register, incident-response runbook, employee onboarding/offboarding policy.
Phase 1.3 — Pre-audit readiness review	T0 + 8 weeks → T0 + 10 weeks	Drata readiness check, mock audit by Drata advisor, last-mile fixes.
Phase 1.4 — Type I audit fieldwork	T0 + 10 weeks → T0 + 14 weeks (Q4 2026)	Auditor engagement, evidence collection, controls testing. Audit report issued ~2 weeks after fieldwork close.
Type I report issued	Q1 2027	Public statement: "SOC 2 Type I attestation issued [DATE] by [Auditor]." Begins Type II observation window.
Phase 2 — Type II observation	Q1 2027 → Q3 2027	Drata continuous-monitoring captures evidence over 6+ months of operation. Quarterly access reviews, annual risk register update, ongoing incident-response drills.
Phase 2.1 — Type II audit fieldwork	Q4 2027	Same auditor engagement; report issued by year-end.
Type II report issued	Q4 2027	Public statement updated.

If seed-close lands at the upper end of the outreach window (8 weeks instead of 6), Type I shifts to Q1 2027 fieldwork / Q2 2027 report, and Type II shifts to Q1 2028.

Vendor selection — Drata

We evaluated three compliance-automation vendors:

Vendor	Year-1 cost	Strengths	Weaknesses	Verdict
Drata	$12–18K	Continuous evidence collection. Mature integrations with our actual stack (GitLab, AWS, Google Workspace, Linear, 1Password). Auditor partner network covers cost-effective firms.	Slightly newer brand recognition than Vanta.	✅ **Selected**
Vanta	$15–20K	Most mature; strongest VC-side brand recognition.	Highest cost; less differentiation for our stack.	Considered.
Secureframe	$10–15K	Cheapest credible option.	Less buyer-side brand awareness; smaller auditor network.	Considered.

Decision rationale: Drata's price-to-capability ratio is best for a seed-stage startup using a GitLab + AWS + Google Workspace stack. Continuous monitoring means Type II evidence accumulates in the background once Type I lands, without re-engagement cycles.

Auditor short-list

Final auditor selection from Drata's partner network within two weeks of seed-close. Working short-list (in alphabetical order; all are Drata-partner firms with multi-year SOC 2 practice):

- A-LIGN
- Coalfire
- Insight Assurance
- Prescient Assurance
- Sensiba San Filippo

Selection criteria:

1. **SaaS-platform-native experience** — auditor has worked with self-hosted-software-shipped-to-customer-perimeter posture, not only managed-SaaS controllers.
2. **Type I → Type II continuity** — same auditor for both reports to minimize re-onboarding cost.
3. **Cost transparency** — flat-fee Type I, no scope-creep surcharges.

Budget (post-seed)

Total Year-1 SOC 2 spend: **$25–38K**.

Line item	Cost band	Source
Drata subscription (Year 1)	$12–18K	Vendor sales engagement
Type I audit fee	$10–15K	Auditor partner from Drata network
DPA template (outside counsel)	$3–5K	Phase 1.1 critical path
Background-check service (first hire onward)	$0 (pre-hire)	First-hire dependency
Optional pen test	$5–10K	Phase 1.4 readiness

This budget is allocated from seed proceeds. No SOC 2 spend pre- seed — the paper artifacts (controls matrix, architecture, privacy, CAIQ Lite, this roadmap) are the entire pre-seed compliance investment and have been delivered free.

Year 2 ongoing cost: ~$15–25K (Drata renewal) + $10–15K (Type II audit fee) + ad-hoc legal updates.

Commitments to customers (the contract)

By executing the standard MSA + DPA, Srasta commits to the following compliance obligations:

1. **Type I attestation by Q1 2027** with a named auditor selected from the short-list above; report shareable under NDA.
2. **Type II attestation by Q4 2027**.
3. **Continuous control operation** during the Type II observation period — outage of a control is a notifiable event, not a private fact.
4. **Customer audit support** — on-prem deployments are audit-friendly: customers can inspect the controls running in their own environment without scheduling Srasta-side access.
5. **Quarterly compliance posture report** to enterprise customers, summarizing controls operated + any deviations.

Public surface (where this commitment shows up)

- `docs/security/soc2-roadmap.md` (this doc) — canonical.
- `docs/security/controls-matrix.md` — referenced from CC1 + CC4 + CC9 rows.
- `docs/legal/privacy-policy.md` — Section 7 references the Type I commitment.
- **Pitch deck v1 (#160)** — the closing slide quotes the one-paragraph commitment verbatim.
- **Website footer** — link to a public-facing summary at `srasta.ai/security` (the page sources from this doc + the controls matrix + the architecture summary).
- **Investor data room** — link to this doc + the controls matrix.

Risks to the timeline

Risk	Mitigation
Seed-close slip beyond 8 weeks	Every milestone shifts by the same amount; commitment paragraph is amended in this doc, not silently.
Drata onboarding delay (vendor-side)	Switch to Vanta as the alternate; both have the same Type I → Type II workflow. ~2-week impact.
Auditor scheduling delay (Q4 2026 is busy)	Lock fieldwork window during Phase 1.1 — book the auditor before Phase 1.2 starts.
Critical CVE during pre-audit window	CI gates already block merge on critical findings; patch + re-deploy via `scripts/upgrade.sh` is on the runbook.
First hire affects HR-domain controls	First hire's onboarding follows the documented procedure produced in Phase 1.2; no scrambling at audit time.

Discipline

- The dated commitment paragraph at the top is **not amended without an explicit edit to this section**. Any communication that quotes a different timeline contradicts our own contract with customers and is a Mandate-3 violation.
- The vendor selection is **not changed** without re-running the decision matrix above and updating this doc.
- The budget line items are **not stretched silently** — if costs exceed the bands above, this doc gets updated and customers/ investors are informed.

Related documents

- `docs/security/controls-matrix.md` — the SOC 2 CC mapping that drives this roadmap's audit scope.
- `docs/security/architecture.md` — the architectural baseline the controls operate against.
- `docs/security/caiq-lite.md` — buyer-questionnaire responses that reference this commitment.
- `docs/legal/privacy-policy.md` — privacy obligations under GDPR / CCPA / DPA.
- `docs/roadmap/compliance-roadmap.md` — long-form compliance roadmap (Phase 0 + Phase 1 + Phase 2); this doc is the seed-stage one-pager that distills its public-facing commitment.
- `docs/strategy/seed-momentum-plan.md` — closure-boundary item #7 (dated SOC 2 Type I commitment).