PanGuard AI — SOC 2 Type 1 Roadmap

For CISO / Compliance Officer review

Updated 2026-05-19

SOC 2 Type 1 Roadmap

Document audience: Compliance officer / CISO evaluating PanGuard AI for procurement.

Status: Pre-audit. Vendor selection complete. Gap assessment in flight.

Target attestation date: Q3 2026 (audit fieldwork July–August 2026, report October 2026).

---

1. Scope

Item	Value
Trust Service Criteria	Security · Availability
Type	SOC 2 Type 1 (point-in-time) — Type 2 to follow in 2027 H1
System boundary	`panguard.ai` (marketing), `app.panguard.ai` (dashboard), `tc.panguard.ai` (Threat Cloud aggregation), and the published `panguard` CLI
Sub-processors in scope	Supabase · Stripe · Vercel · Cloudflare · Sentry · Anthropic (build-only) · Fly.io · GitHub · Google Workspace (full list at panguard.ai/sub-processors)
Data classes covered	Customer workspace data, anonymised telemetry, audit logs

Type 1 is the right starting attestation because the company is < 12 months old in C-Corp form (Panguard AI Inc. filed 2026-05-12) — Type 2 requires a 6- to 12-month observation window. Most enterprise buyers accept Type 1 + a Type 2 commitment letter for first-year Pilot contracts.

---

2. Vendor & auditor selection

Compliance automation platform

Vendor	Status	Reason
Vanta	**Selected**	Best fit for early-stage AI infra. Native integrations with Supabase, GitHub, Stripe, Sentry, Fly.io. SOC 2 + ISO 27001 dual-track.
Drata	Evaluated, runner-up	Heavier in policy management; less mature for AI-specific controls.
Secureframe	Evaluated	Strong but Vanta partner-list better matched our stack.

Vanta contract target: **2026-06-01**. Onboarding + integration sweep: **2026-06-01 □ 2026-06-15**.

Independent CPA auditor

Auditor	Status
A-LIGN	Primary candidate. Cyber-native CPA firm. ~$25K SOC 2 Type 1.
Prescient Assurance	Backup candidate. ~$18K but smaller team.
BDO USA	Considered, declined — too expensive for early stage.

Auditor engagement letter target: **2026-06-30**. Fieldwork: **2026-07-15 □ 2026-08-31**.

---

3. Timeline

```
2026-05-12    Panguard AI Inc. (Delaware C-Corp) filed via Stripe Atlas
2026-05-19    Vendor selection (Vanta + A-LIGN candidate list locked)  ← TODAY
2026-06-01    Vanta contract signed · onboarding begins
2026-06-15   Vanta integrations live (Supabase / GitHub / Sentry / Stripe / Fly.io)
2026-06-30    Gap assessment complete · remediation backlog filed
2026-07-15    Auditor engagement letter executed (A-LIGN preferred)
2026-07-15 ── 2026-08-31    Audit fieldwork
2026-09-15    Draft Type 1 report
2026-10-01    SOC 2 Type 1 attestation issued        ← target deliverable
2026-12-01    Continuous-monitoring window opens for Type 2
2027-04-01    SOC 2 Type 2 audit fieldwork begins
2027-06-30    SOC 2 Type 2 attestation issued
```

---

4. Control families & current state

4.1 Access control

- Magic-link authentication via Supabase Auth (email-only). MFA via emailed one-time code.
- Workspace-level RLS on every database table. Service role keys held in Vercel/Fly secret managers, never committed.

- Production database admin access: 1 person (founder), audit-logged via Supabase audit_logs table.
- **Gap to close:** SAML SSO for Enterprise tier (target Q3 2026, ships alongside the audit).

4.2 Encryption

- TLS 1.3 everywhere (Cloudflare in front of every public surface).
- Database at-rest: Supabase managed Postgres, AES-256 disk encryption (their SOC 2 in inheritance chain).
- Secrets: Stripe / Anthropic / Sentry tokens stored in Vercel env, marked production-only.
- **Gap to close:** customer-managed encryption keys (CMEK) — Enterprise feature, target Q4 2026.

4.3 Vulnerability management

- Dependabot + GitHub security advisories enabled, automatic PR for high/critical CVEs.
- `pnpm audit --audit-level high` runs in CI on every push.
- Third-party penetration test: **not yet engaged.** Scheduled with audit fieldwork (Vanta vetted vendor list).
- Annual pen-test commitment in writing — included with Enterprise contract.

4.4 Incident response

- 72-hour breach notification SLA in DPA (panguard.ai/legal/dpa).
- security@panguard.ai 24/7 monitored (forwards to PagerDuty after-hours).
- Incident runbook lives in private internal repo, sample sanitised redaction shareable under NDA.

4.5 Vendor risk

- Sub-processor list maintained at panguard.ai/sub-processors with 30-day customer-notice clause.
- All sub-processors hold SOC 2 Type 2 (Supabase / Stripe / Vercel / Cloudflare / Anthropic / Fly.io) — inheritance documented in the audit work paper.

4.6 Logical separation

- Workspace isolation: every row in every table carries `workspace_id`. RLS policy enforces equality with the JWT claim. Cross-workspace reads provably impossible at the database layer.
- Threat Cloud telemetry: only anonymised fingerprints (SHA-256 + severity) leave the customer environment. Customer skill content never transmitted.

---

5. What this means for a Pilot contract today

A 90-day Pilot ($25K) can sign today **before** the Type 1 attestation, on the strength of:

1. The published security whitepaper at panguard.ai/legal/security (this document, plus 6 more sections).
2. The signed DPA at panguard.ai/legal/dpa (GDPR + Taiwan PDPA compliant).
3. The sub-processor list with 30-day notice clause.
4. A signed Type 1 commitment letter (issued by founder on letterhead, delivery date Oct 1 2026).
5. NDA-gated access to: architecture diagrams, threat model, audit log samples, Vanta dashboard read-only.

Enterprise contracts ($150K+) execute alongside or after the Type 1 attestation. Pilot customers automatically receive a copy of the final attestation report when issued, and may convert their Pilot fee against the Y1 Enterprise contract.

---

6. Contact

Document owner: Adam Lin, founder & compliance lead **Email:** security@panguard.ai **PGP:** panguard.ai/.well-known/pgp-key.txt **Office:** Taipei, Taiwan (US C-Corp; sub-processors operate in stated jurisdictions)

For NDA + dashboard read-only access during Pilot evaluation, contact security@panguard.ai with subject line `[SOC2 Eval] <Your Org Name>`.

Confidential — provided to evaluators for procurement review. Do not redistribute.