COMPLIANCE · TEMPLATE

Vanta vs. Drata vs. Doing It Yourself: SOC 2 Automation *Compared*

KAANSYSTEMS.COM/LIBRARY/VANTA-VS-DRATA-SOC2 · SEPTEMBER 16, 2026

ABOUT THIS TEMPLATE

Vanta and Drata both auto-collect SOC 2 evidence from your stack; the differences are marginal. Pick by integration coverage, auditor, and price — not brand.

THE TEMPLATE

Score each item honestly before you sign anything. This is a selection scorecard, not a checklist to complete — it tells you which column you are in.

Step 1 — Are the controls actually in?

- ☐ SSO fronts every SaaS tool that supports it; MFA enforced on 100% of accounts
- ☐ Prod and dev are separated (accounts or hard boundaries), not sharing one blast radius
- ☐ Change management is real: reviewed PRs through a gated pipeline with traceable history
- ☐ Logging is centralized and tamper-resistant
- ☐ Offboarding is a single revocation action

If most of these are `no`, no platform helps yet — the subscription would rent you a view of the backlog. Build the controls first (or run a readiness sprint), then come back to this template.

Step 2 — Coverage: trial both read-only for a week

- ☐ Listed every system that must produce evidence: IdP, cloud accounts, code host, MDM, HR, ticketing
- ☐ Confirmed each platform has a native connector for each — no gaps handled by manual upload
- ☐ Recorded, per platform, the percentage of controls evidenced automatically vs. manually for YOUR stack

- [ ] Verified framework coverage for what you need in the next 24 months (SOC 2, and ISO 27001 / HIPAA / GDPR if on the roadmap)

Step 3 — Auditor

- [ ] Confirmed your preferred audit firm works on the platform, or picked one from its marketplace
- [ ] Got a fee range from firms that completed audits on the platform in the last 12 months
- [ ] Confirmed you can bring your own auditor if you want to

Step 4 — Price the future, not the present

- [ ] Year-two list price in the order form, not the sales thread
- [ ] Employee-tier boundaries documented (what happens if you cross 50 / 100 mid-contract)
- [ ] Multi-framework add-on price locked in writing at initial signature
- [ ] At-churn export terms confirmed: evidence history, format, retention

Step 5 — The DIY sanity check

- [ ] A named engineer would own the evidence pipeline as real, staffed work (not "the team")
- [ ] Scope is either a tiny first Type I or a team already running durable, queryable log storage
- [ ] You have accepted that manual collection decays past ~20 controls and re-runs every Type II quarter

If Step 5 is mostly true, DIY is viable and you can skip the subscription. Otherwise, whichever platform won Step 2 for your stack is the answer — and the margin between Vanta and Drata is small enough that either is a defensible call. Buy on coverage, auditor, and renewal price; then go build the controls, because that is the part no tool does for you.

WHAT DO VANTA AND DRATA ACTUALLY DO?

The same thing, competently. Both are evidence-automation platforms: read-only connectors reach into your identity provider, your cloud accounts, your source host, your MDM, and your HR system, and pull compliance evidence automatically and continuously — MFA status per user, encryption settings per bucket, branch protection per repo, offboarding timestamps per departure. That evidence gets mapped to the SOC 2 Common Criteria (and to ISO 27001, HIPAA, or other frameworks if you scope them), tracked against control owners with deadlines, and surfaced on an auditor-facing dashboard so your CPA firm reads evidence in the tool instead of over email attachments.

That is the product, and it is genuinely valuable. Manual evidence collection for a SOC 2 cycle runs 50 to 100-plus hours of mostly senior engineer time, all of it miserable, and it has to be redone every cycle because auditors need evidence from the current period. A platform does that collection on a schedule, forever.

Continuous monitoring is the second real benefit: a control that silently degrades in March surfaces in March, not during next January's fieldwork.

Vanta and Drata are the two market leaders, but they are not the only credible options — Secureframe, Thoropass, and Sprinto do the same job and are worth a quote, especially if one of them has better coverage for your particular stack. The category matters more than the logo.