COMPLIANCE · TEMPLATE

Do You Need a Compliance Platform? Vanta, Drata, and the *Honest* Answer

KAANSYSTEMS.COM/LIBRARY/DO-YOU-NEED-A-COMPLIANCE-PLATFORM · SEPTEMBER 2, 2026

ABOUT THIS TEMPLATE

Vanta and Drata automate evidence collection; they do not implement controls. When DIY, platform-only, or engagement-first actually wins.

THE TEMPLATE

Score each factor 0 to 2. Total honestly; the bands below do the rest.

Part 1: score yourself

#	FACTOR	0 POINTS	1 POINT	2 POINTS
1	**Controls implemented** (of these five: SSO + enforced MFA; prod/dev account separation; documented and followed change management; offboarding within 24h; centralized logging)	0-1 of 5 running	2-3 of 5	4-5 of 5
2	**Internal owner**	Nobody named	Named, under 10% of their time	Named, 25%+ time protected
3	**Timeline runway**	Report needed inside 4 months; deal blocked now	4-8 months	8+ months
4	**Frameworks needed, next 24 months**	One-time Type I only	SOC 2 Type II, annually	Type II plus HIPAA / ISO / others
5	**Year-one budget** (software + outside help, excluding auditor fee)	Under $5k	$5-20k	$20k+

Part 2: read the bands

```
GATE RULE (evaluate first):
  Q1 ⩽ 1 AND Q2 ⩽ 1  →  ENGAGEMENT FIRST, THEN PLATFORM.
      No purchase fixes an unstaffed readiness gap. Q3 = 0 makes
      this more true, not less: urgency without capacity is the
      exact case outside help exists for.

  Q1 ⩽ 1 AND Q2 = 2   →  INTERNAL READINESS WORK FIRST.
      Run the sprint yourselves. Buy the platform when Q1
      would score 2. Trial it now for the gap list (free).

IF Q1 = 2 (controls are in):
  Q4 = 0 AND Q5 = 0    →  DIY IS VIABLE.
      First Type I, tiny scope, near-zero budget. Accept the
      100-150 hours and know DIY does not survive a Type II
      observation window.

  Otherwise            →  PLATFORM NOW.
      Evidence automation is your actual bottleneck. Buy it,
      pick an auditor, open the window.
```

Part 3: questions to ask the platform vendor

01 Walk through the connector for each of our systems by name: IdP, cloud accounts, MDM, repo host, ticketing. Which of our controls have no connector coverage?

02 For our exact stack, what percentage of this framework's controls will be evidenced automatically versus manual upload?

03 Can we bring our own audit firm? Which firms completed audits on your platform in the last 12 months, and at what fee range?

04 What does adding HIPAA or ISO 27001 cost at renewal, and how much of our SOC 2 evidence actually maps across?

05 Where exactly are the price step-ups: employee tiers, framework count, connector count? What happens if we cross a tier mid-contract?

06 What does the access-review workflow do beyond scheduling and reminders?

07 At churn, what do we get out: evidence history, format, retention?

08 What will the year-two renewal say, at list, if nothing about us changes?

—— HOW TO USE IT

Run the trial as a free gap assessment

Connect the trial read-only, let it scan everything, and export the red list before the trial expires. That list is a legitimate readiness assessment, the kind consultancies charge five figures for, and you are allowed to take it and walk. The vendors know this and price it into the funnel. Signing before the list is mostly green, or before there is a funded plan to make it green, is the mistake this entire article is about.

Green is not the same as compliant

The platform checks what its connectors can see. An auditor samples beyond that: they interview your engineers, pull real tickets, and read your policies against your actual behavior. A policy library adopted in one click that describes a change process nobody follows is worse than no policy, because now the gap is documented. Treat the dashboard as necessary telemetry, not as the audit result. Type II reports are built from operating effectiveness over months, and no connector attests to culture.

The renewal is where the price lives

Year-one pricing is a land grab; year two is the business model. Before signing, get the multi-framework add-on price, the employee-tier boundaries, and the year-two list price in the order form, not the sales thread. Teams that negotiate the HIPAA add-on at initial signature routinely pay half what teams pay when they add it at renewal, for the obvious reason: by renewal, your evidence history lives there, and the vendor knows what migration costs you.