COMPLIANCE · TEMPLATE

Choosing Between SOC 2, HITRUST, and HIPAA Attestation

KAANSYSTEMS.COM/LIBRARY/CHOOSING-SOC2-HITRUST-HIPAA · MAY 30, 2026

ABOUT THIS TEMPLATE

Three certifications, three different signals, three different buyers. A decision matrix: what each one actually costs, what each one actually proves, and which one your buyers actually need.

THE TEMPLATE

Use this cheat-sheet to make the decision:

Step 1: Identify your top 3 active deals (or top 3 target accounts).

Step 2: For each, find their security requirements in writing. Either ask the buyer, or look at their published vendor security expectations.

Step 3: Tally which frameworks appear:

- SOC 2: ____ deals
- HITRUST: ____ deals
- HIPAA assessment: ____ deals
- ISO 27001: ____ deals
- Other: ____ deals

Step 4: Apply the rule: pursue the framework that unblocks the most current revenue. If the tally is unclear, default to SOC 2 first — it has the broadest applicability and the most reusable artifacts.

Step 5: Set a realistic timeline. Most teams over-commit on the first cycle. Add 30% buffer to the auditor's estimate.

Step 6: Budget for it — both dollars and internal time. The single most common reason compliance projects fail is that internal time gets reallocated to product work mid-cycle.

HOW TO USE IT

Don't pursue all three frameworks at once. The artifacts overlap heavily (a control documented for SOC 2 is 80% reusable for HITRUST), but the audit cycles and assessor relationships are distinct. Trying to run two cycles simultaneously in a team of fewer than 100 engineers usually means both slip.

The first framework you obtain is the expensive one. Subsequent frameworks share the readiness work — the policies, the evidence pipelines, the security training program, the vendor management process all carry forward. Plan as if SOC 2 → HITRUST is half the work of SOC 2 alone.

The framework you have is less important than the operating muscle you build around it. The team that meaningfully runs SOC 2 — quarterly access reviews, monthly evidence collection, annual control updates — is the team that will pass HITRUST easily. The team that scrambled to pass SOC 2 once and forgot about it will fail HITRUST and then fail SOC 2 renewal.

Compliance is a continuous practice, not a project.