

State of Startup Security 2026

What 130 early-stage startups show enterprise buyers in public, what SOC 2 and ISO 27001 really cost, and a 90-day plan to close the gap.

130 startups reviewed from public signals only

47% score 4 or less out of 10

9 of 130 publish a DPA we could open

Inside: benchmark data by sector, region and stage · SOC 2 and ISO 27001 cost breakdown · Type I vs Type II timelines · The 20 questions buyers ask · 30-60-90 day plan · One-page self-assessment

Free to share with attribution · grcompliance.com

Key findings

In October 2026 we reviewed the public websites of 130 startups that recently raised pre-seed to Series B rounds or are publicly hiring for security and compliance. We checked the ten things an enterprise buyer's security reviewer looks for before the first call. We did not contact anyone, log in, or scan anything. We only read what any buyer can see.

4.6 mean score out of 10 (median 4.5)	47% are 'Early' (score ≤ 4)	13% are 'Advanced' (score ≥ 7.5)	2.37/6 security headers on the average homepage
--	--	---	--

- 1. Most startups are not buyer-ready in public.** 61 of 130 (47%) score 4 or less out of 10. Only 17 (13%) reach 7.5. The median is 4.5.
- 2. There is a 'claim gap'.** 73 companies (56%) mention SOC 2 or ISO 27001 somewhere. 15 of them have no findable security or trust page to back it up, and only 5 publish a DPA we could open.
- 3. The legal paperwork is the weakest area.** A privacy policy is near-universal (85%). A public subprocessor list (28%) and a readable DPA (7%) are rare, yet GDPR Article 28 makes both standard asks from EU buyers.
- 4. The cheapest fixes are the most skipped.** Only 5 companies (4%) publish a valid security.txt, which is a 15-minute job. Only 6 send all six basic security headers. 34% have a public status page.
- 5. Funding stage barely matters. Starting the work does.** Seed companies average 4.21 and Series A/B 4.72. The small group publicly working on SOC 2 averages 7.0.
- 6. Marketing trackers usually run before consent.** 108 homepages (83%) load marketing or analytics trackers. On 33 of them we detected no consent banner or consent tool. 36 load person-level visitor-identification tools.

What it costs to fix: a first SOC 2 Type II typically costs a 10–25 person startup about \$25k–\$50k in cash in year one, before internal time (Drata). The fastest realistic path to a Type II report is about 6–7 months, because the auditor has to observe your controls working for a period of at least 3 months. Details on pages 10–12.

Free: your own Readiness Snapshot

We will run the same 10 public checks on your domain and send a one-page snapshot with your score, your top 5 gaps and what to fix first. It is free, passive, and does not need system access. Reply to this report or visit grcompliance.com.

Contents

#	Section	Page
1	Key findings	2
2	The 10 signals buyers check	4
3	Findings: overall	5
4	Findings by sector, region and stage	7
5	Privacy and security hygiene	9
6	What SOC 2 and ISO 27001 really cost	10
7	Timelines: Type I, Type II and ISO certification	12
8	The 20 questions enterprise buyers actually ask	13
9	30-60-90 day readiness plan	15
10	Quick wins you can ship this week	16
11	One-page self-assessment	17
12	Method and limitations	18
13	Sources and about GRCompliance	19

Who this is for

- Founders and CTOs at seed to Series B B2B companies who are starting to sell to mid-market and enterprise buyers.
- The first security, compliance or RevOps hire who has been handed a security questionnaire and a deadline.
- Investors and advisors who want a quick benchmark for portfolio companies.

How to use it

Use pages 4–9 to benchmark yourself against peers. Use pages 10–12 to budget and plan. Pages 13–17 are the working tools: the 20 buyer questions, a 90-day plan, a list of quick wins and a one-page self-assessment you can print and fill in today. Every number in this report comes either from our own public-signal review (described on page 18) or from a cited public source (page 19).

Scoring, in one line: each of the 10 signals is Found (1 point), Partial (0.5) or Missing (0). Early = 4 or less, Developing = 4.5 to 7, Advanced = 7.5 or more. This is a measure of how much buyer-grade evidence is visible, not of how secure a company actually is.

2. The 10 signals buyers check

Before a buyer's security team sends a 200-question spreadsheet, someone usually spends ten minutes on your website. These are the ten things they look for, and why each one matters.

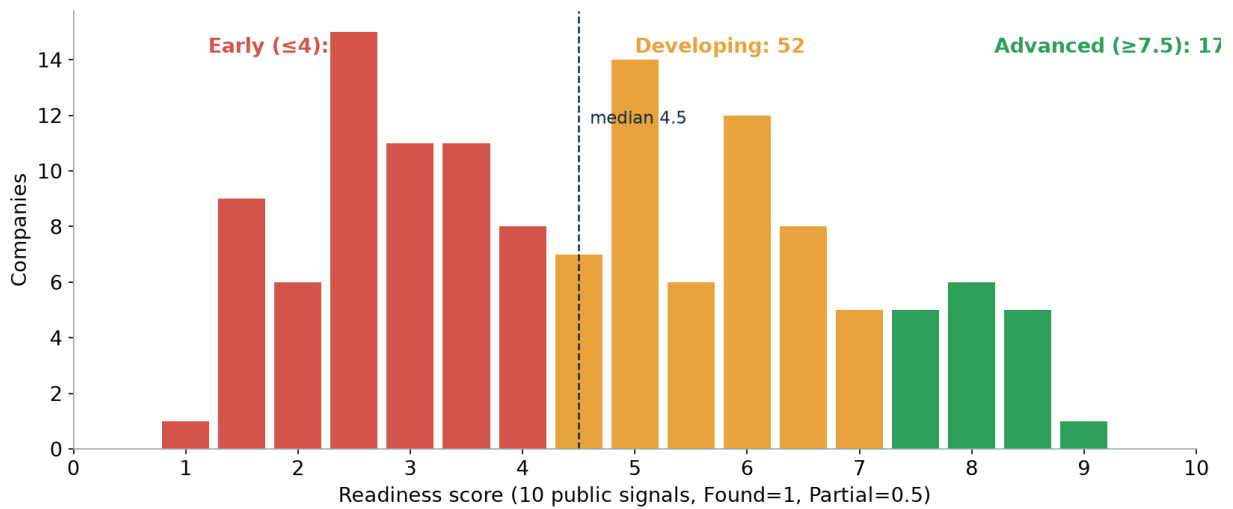
#	Signal	Why buyers care	What 'Found' means
1	Security / trust page	A page describing your controls, or a trust centre. This is where reviewers start.	Has real content: encryption, access, incident response, testing
2	SOC 2 / ISO evidence path	A claim the buyer can verify: a report-request flow, certificate or trust-centre entry.	A badge with no way to get the report scores Partial
3	Privacy policy	A baseline legal requirement and the first link a reviewer clicks.	Specific, current, names the data controller
4	Subprocessor list	GDPR Art. 28 and most DPAs require you to disclose sub-processors and notify changes.	Public list naming vendors, purpose and region
5	DPA available	EU and UK buyers need a Data Processing Agreement before any personal data flows.	Downloadable or click-through DPA
6	security.txt / disclosure	RFC 9116 file telling researchers how to report issues to you.	/.well-known/security.txt with Contact and Expires
7	Security headers	Visible hygiene: HSTS, CSP, X-Frame-Options, nosniff, Referrer-Policy, Permissions-Policy.	5 or more of 6, including HSTS
8	SSO / MFA documented	Enterprise IT will ask for SAML SSO (and often SCIM) and MFA.	Both SSO and MFA mentioned in docs, pricing or the security page
9	Status page	Shows uptime and incident history, which supports availability claims.	Public status page linked from the site
10	Cookie consent	Trackers before consent is a visible GDPR/ePrivacy issue.	A consent tool, or no trackers at all

Signal set mirrors common opening questions in the CSA CAIQ v4 / Cloud Controls Matrix (17 domains, 197 control objectives) and the Shared Assessments SIG, plus RFC 9116 and OWASP Secure Headers guidance.

3. Findings: overall

47% of funded startups score 4 or less out of 10

Distribution of public trust-signal scores, mean 4.6 / median 4.5

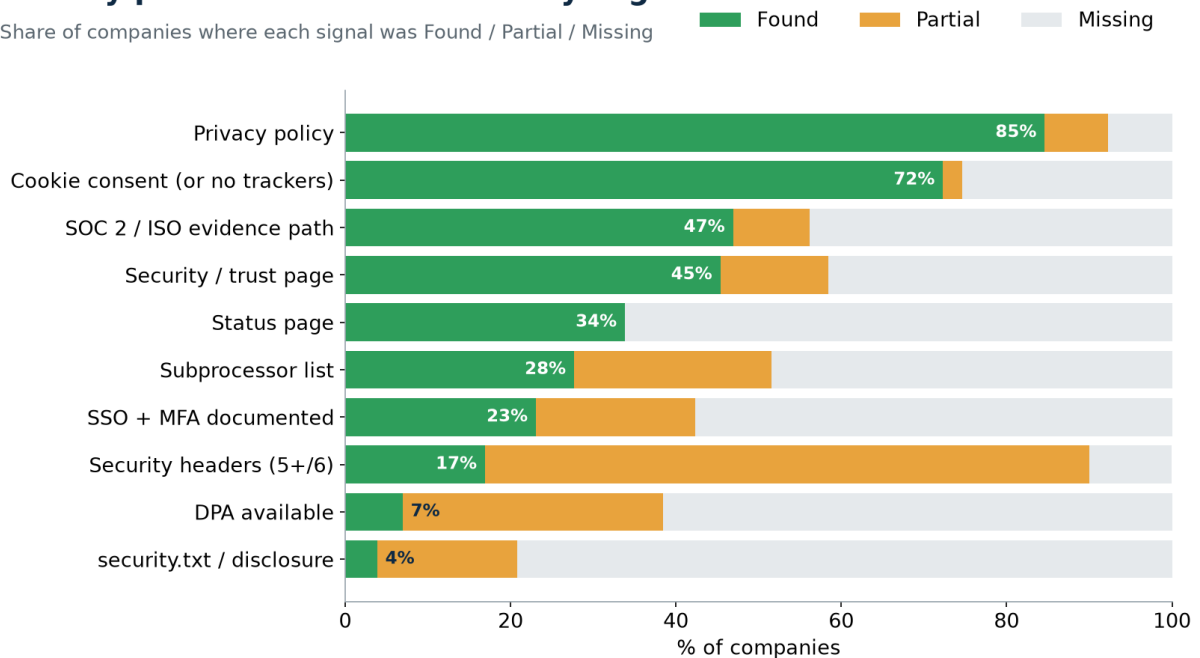


Source: GRCompliance passive public-signal review, Oct 2026, n=130 startups. Not an audit. grcompliance.com

The distribution has two humps. About half the companies sit around 2–4: they have a privacy policy and a cookie banner, and not much more. The other half cluster at 5–6: they have a security page and mention SOC 2, but are missing the legal paperwork (DPA, subprocessors) and the hygiene signals (security.txt, headers). Only 17 companies cover nearly all ten.

Privacy policies are universal. Buyer-grade evidence is not.

Share of companies where each signal was Found / Partial / Missing



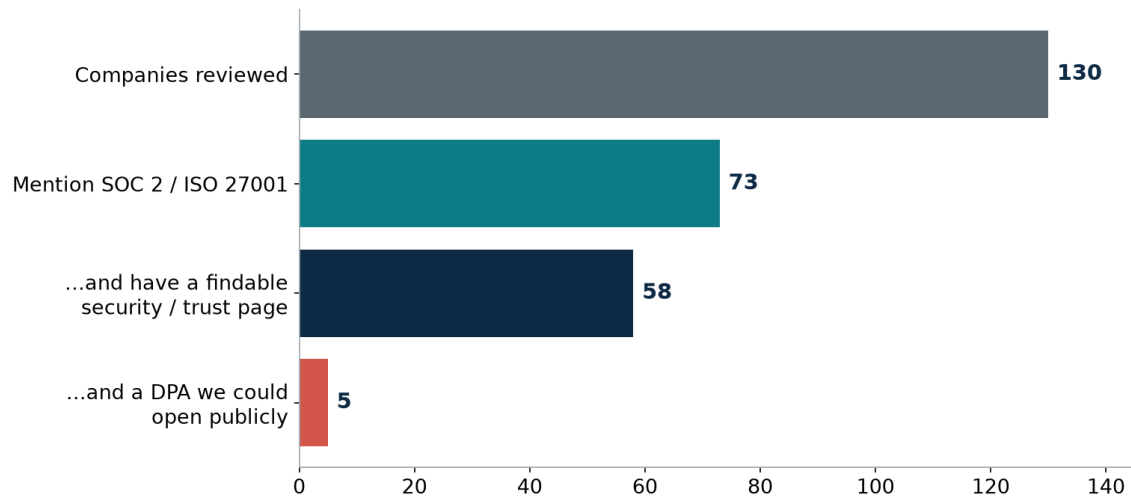
Source: GRCompliance passive public-signal review, Oct 2026, n=130 startups. Not an audit. grcompliance.com

Read this chart from the bottom up. The four least common signals are security.txt (4%), a readable DPA (7%), full security headers (17%) and documented SSO + MFA (23%). Three of those four take less than a day to fix.

The claim gap

Of 73 companies that mention SOC 2 or ISO, only 5 publish a readable [

The 'claim gap': a badge on the homepage is not the evidence a buyer's procurement team asks for



Source: GRCompliance passive public-signal review, Oct 2026, n=130 startups. Not an audit. grcompliance.com

Mentioning SOC 2 is now common: 56% of companies do it. But a reviewer's next three requests are predictable: the report (or a bridge letter), the DPA and the subprocessor list. Most companies that mention SOC 2 make the reviewer ask for all three by email, which adds days to every deal. 15 companies mention SOC 2 or ISO with no security or trust page at all. This is the pattern most likely to raise a reviewer's suspicion rather than lower it.

What good looks like: a single trust page that states your framework status honestly (for example "SOC 2 Type II observation period ends March 2027"), offers the report under NDA, and links to the DPA, the subprocessor list, the status page and security.txt. That one page answers the first five questions of most questionnaires.

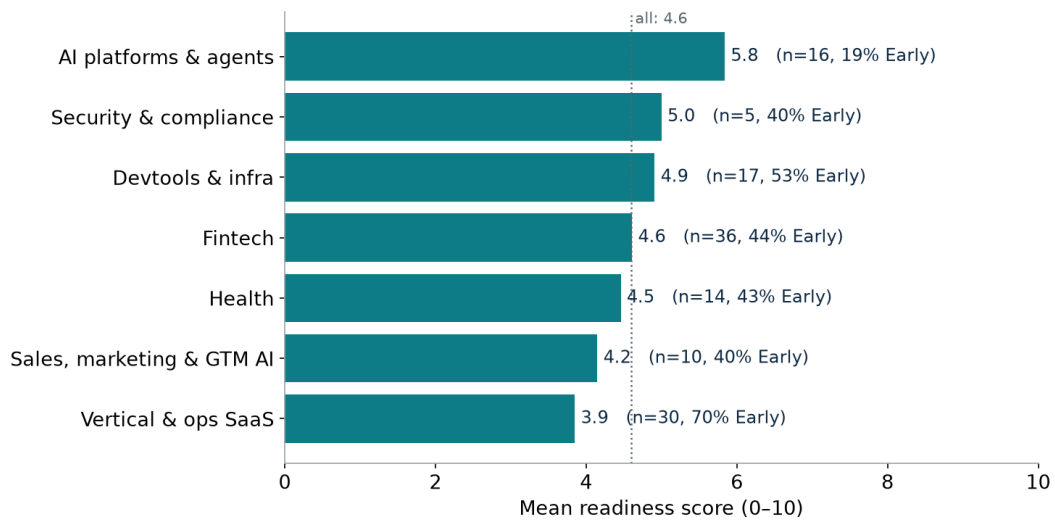
Questionnaire on your desk right now?

Our Security Questionnaire Service completes SIG Lite, CAIQ and custom spreadsheets from the controls you actually run, and flags gaps honestly. Express \$750 (up to 100 questions, 48 hours) · Standard \$1,500 (up to 300) · Retainer \$2,500/month. See grcompliance.com/pricing.html.

4. Findings by sector, region and stage

No sector is enterprise-ready by default

Mean score by sector (sectors with $n \geq 4$). Sector assigned from public descriptions.



Source: GRCompliance passive public-signal review, Oct 2026, $n=130$ startups. Not an audit. grcompliance.com

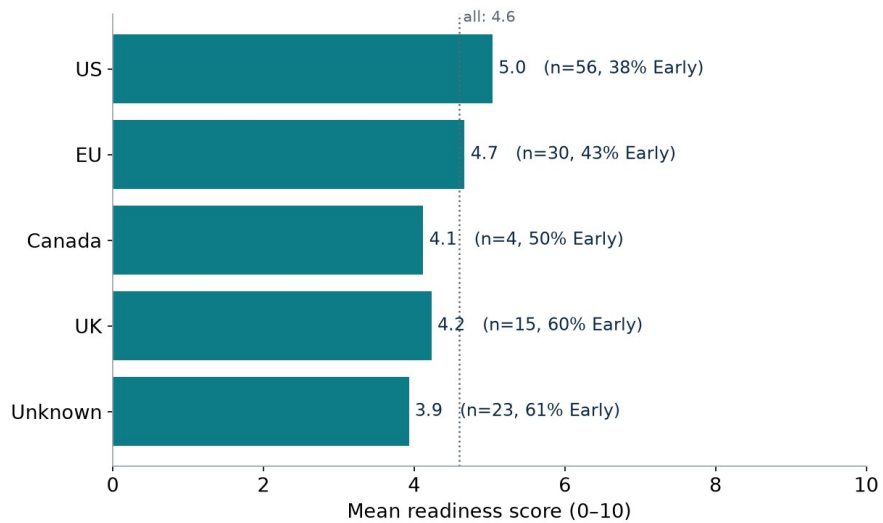
Sector	n	Mean	Early	SOC 2/ISO mentioned	Trust page	Subproc. list	DPA
Fintech	36	4.61	44%	56%	44%	25%	8%
Vertical & ops SaaS	30	3.85	70%	43%	27%	30%	10%
Devtools & infra	17	4.91	53%	47%	47%	24%	6%
AI platforms & agents	16	5.84	19%	81%	75%	50%	0%
Health	14	4.46	43%	64%	43%	29%	0%
Sales, marketing & GTM AI	10	4.15	40%	50%	50%	20%	20%
Security & compliance	5	5.0	40%	80%	60%	0%	0%

AI platform companies score highest (5.84). They sell to enterprise data and IT teams from day one, and trust pages have become standard in that category. Vertical and operations SaaS (construction, logistics, energy, procurement and so on) scores lowest, with 70% Early, even though these companies often sell to large incumbents with strict procurement. Fintech (4.61) and health (4.46) sit at the average, which is lower than their regulated buyers will expect.

Sector assigned from public company descriptions. Segments with fewer than 4 companies are not shown separately.

Region matters less than you'd think

Mean score by HQ region inferred from public info (Unknown = not determinable)

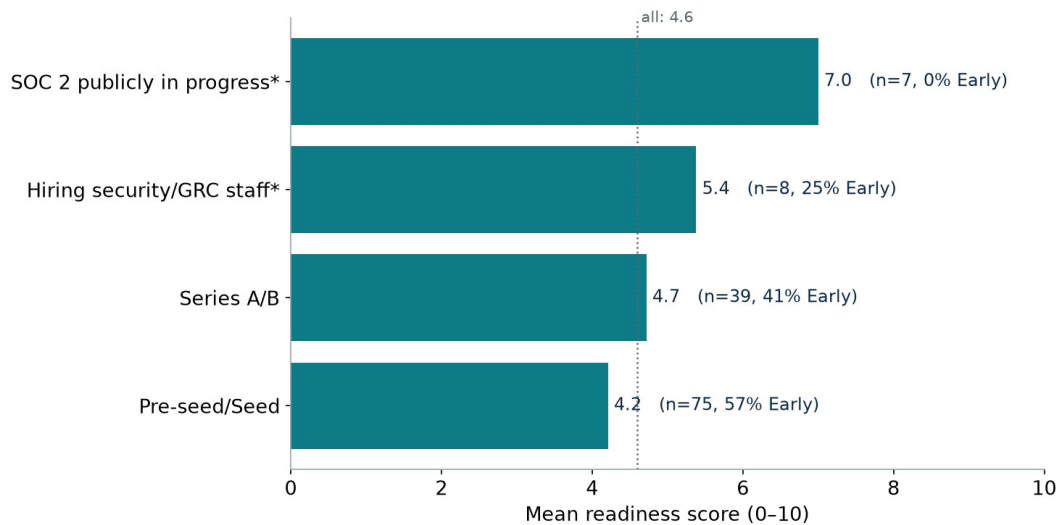


Source: GRCompliance passive public-signal review, Oct 2026, n=130 startups. Not an audit. grcompliance.com

US companies score a little higher (5.04, n=56) than EU (4.67, n=30) and UK companies (4.23, n=15). The gap is mostly SOC 2 mentions and trust centres, which are US-buyer conventions. EU companies are slightly more likely to publish a DPA (13% vs 5% in the US), but the numbers are low everywhere. If you are a European startup selling to US enterprises, expect SOC 2 to be asked for even if you hold ISO 27001.

Series A barely moves the score. Starting the work does.

Mean score by funding stage, and for two small trigger cohorts (*n<10, directional only)



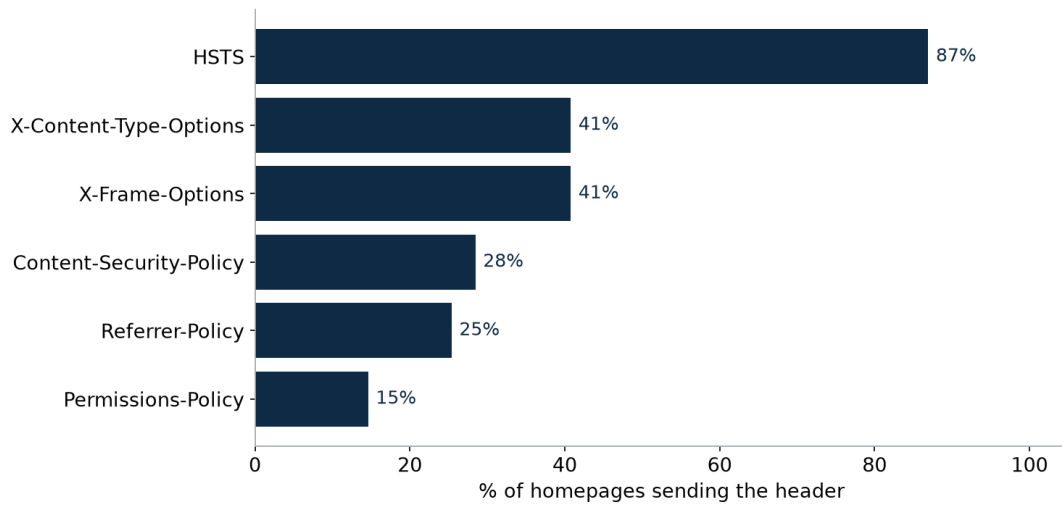
Source: GRCompliance passive public-signal review, Oct 2026, n=130 startups. Not an audit. grcompliance.com

Series A/B companies average only about half a point more than seed companies (4.72 vs 4.21). A bigger round does not by itself produce trust artefacts. The two small trigger groups are different: companies that publicly say SOC 2 is in progress average 7.0, and none of them are Early. The groups are small (7–8 companies each), so treat this as directional.

5. Privacy and security hygiene

Average homepage sends 2.37 of 6 basic security headers

Only 6 of 130 send all six. Most of these are a 10-minute config change.

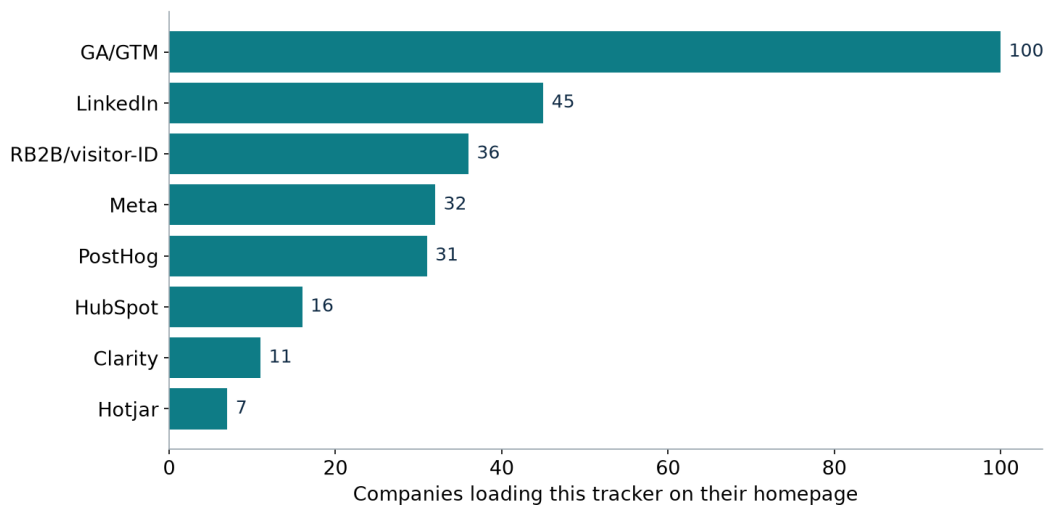


Source: GRCompliance passive public-signal review, Oct 2026, n=130 startups. Not an audit. grcompliance.com

HSTS is common (87%) because most modern hosting platforms send it by default. Everything else must be configured deliberately, and most teams never do it: Content-Security-Policy 28%, Permissions-Policy 15%. Reviewers and automated vendor-risk tools (security rating services) check these headers, and the fix is usually a few lines in your CDN, framework or hosting config.

108 of 130 homepages load marketing trackers; 33 show no consent mechanism

Trackers detected in homepage HTML/JS. 'Visitor-ID' = person-level de-anonymisation tools.



Source: GRCompliance passive public-signal review, Oct 2026, n=130 startups. Not an audit. grcompliance.com

Google Analytics/Tag Manager appears on 100 homepages, LinkedIn's Insight Tag on 45, and person-level visitor-identification tools on 36. A privacy-conscious buyer, especially in the EU, will notice trackers firing before consent. Visitor-identification tools are a particular risk to mention honestly in a DPA or privacy review.

6. What SOC 2 and ISO 27001 really cost

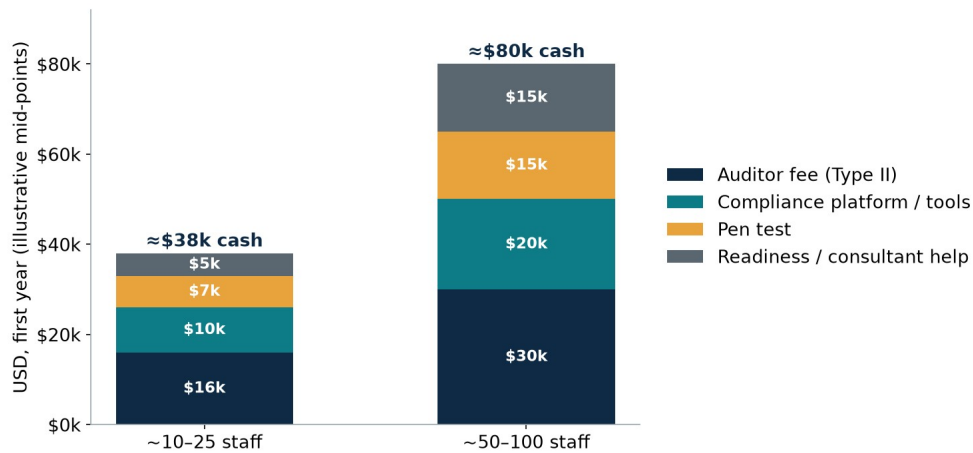
The audit fee is the line item founders ask about, but it is rarely the biggest cost. The figures below are ranges published by compliance vendors, pen-test firms and ISO certification guidance. They are planning numbers, not quotes.

SOC 2: first-year cost by company size (USD)

Line item	~10–25 staff	~50–100 staff	250–500+ staff	Public source
Auditor fee, Type I	\$7.5k–\$15k	\$7.5k–\$15k	\$20k–\$60k	Drata
Auditor fee, Type II	\$12k–\$20k	\$15k–\$35k	\$30k–\$100k+	Drata \$12k–\$20k (small/mid), \$30k–\$100k+ (large); Vanta: most fees \$10k–\$50k
Readiness / gap assessment	\$5k–\$10k	\$10k–\$25k	\$25k+	Drata \$5k–\$25k; Vanta from ~\$10k
Compliance platform & security tools	~\$10k	\$10k–\$25k	\$25k–\$50k+	Vanta ~\$10k tools; Drata \$5k–\$50k+
Penetration test (web app + API)	\$5k–\$9k	\$9k–\$20k	\$20k–\$35k+	Blaze 2026 pricing guide
Consultant / policy help (optional)	\$0–\$10k	\$5k–\$25k	\$25k+	Drata \$5k–\$25k+
Internal people time	Hundreds of hours	0.25–0.5 FTE for 3–6 mo.	Dedicated GRC team	Drata, Vanta: largest hidden cost
Typical first-year cash total	~\$25k–\$50k	~\$75k	~\$180k+	Drata scenarios (25 / 100 / 500+ staff)
Ongoing per year	\$15k–\$40k	\$25k–\$60k	\$100k+	Drata: \$15k–\$40k to maintain

What a first SOC 2 Type II really costs (before your team's time)

Mid-points of published ranges. Internal people time is the biggest hidden cost and is not shown.



Sources: Drata, Vanta, Blaze Information Security public pricing guides (2026). Illustrative, not a quote. grcompliance.com

Where a source gives one range for 'small to midsize', we used it for both smaller columns. FTE estimate is a GRCompliance planning assumption, not a vendor figure.

ISO 27001: certification audit cost by headcount (UK, GBP)

ISO 27001 audit time is not negotiable in the way people assume. Certification bodies work from the audit-day table in ISO/IEC 27006-1, which sets days by the number of people in scope. Bodies may adjust by up to 30% for complexity. Each year you also have a surveillance audit (about a third of the initial days), and in year three a recertification audit (about two thirds).

People in scope	Audit days (Stage 1+2)	Certification audit	Each surveillance audit	Preparation (consultant-led)	First 3 years total
10	5	£5,500–£7,500	£1,850–£2,500	£3,600–£16,800	£12,800–£29,300
25	7	£7,700–£10,500	£2,550–£3,500	£6,000–£26,400	£18,800–£43,900
60	10	£11,000–£15,000	£3,650–£5,000	£12,000–£54,000	£30,300–£79,000
150	13	£14,300–£19,500	£4,750–£6,500	£18,000–£78,000	£41,800–£110,500

Audit days from ISO/IEC 27006-1:2024 Table C.1 as reproduced by iso27001partners.co.uk. GBP figures are that publisher's estimates at £1,100–£1,500 per auditor day, excluding VAT and travel. You also need an independent internal audit every year (ISO 27001 clause 9.2), which your certification body cannot provide.

Where the money actually goes

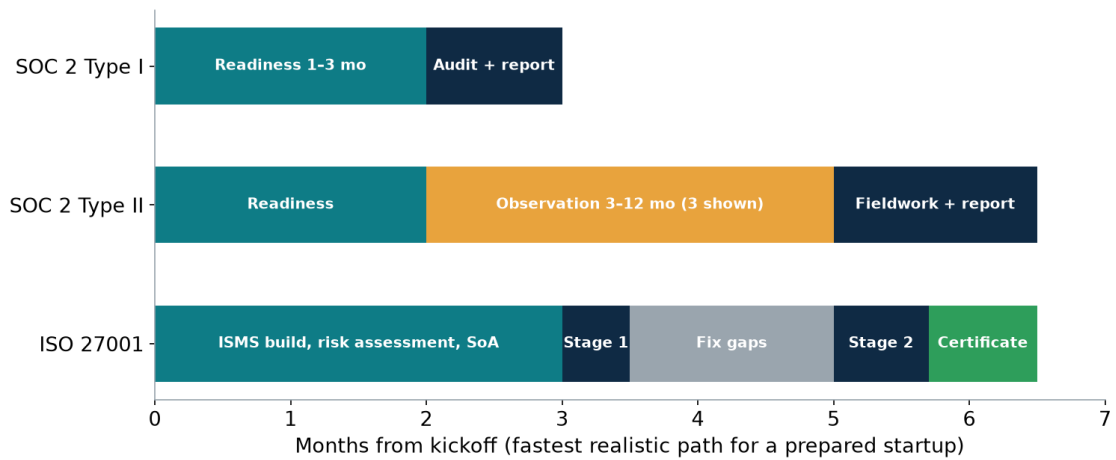
- People time is the largest cost. Both Drata and Vanta call internal time the biggest hidden cost. It is mostly engineers collecting evidence and changing configurations.
- Type I first can mean paying twice. Vanta notes that many buyers now want Type II specifically. Buy a Type I only if a named deal will accept it now.
- Scope is the biggest lever. Keep SOC 2 to the Security criterion unless a contract requires more, and draw the ISO scope around the product you actually sell.
- Choose an auditor sized for startups. Boutique CPA firms cost a fraction of Big Four fees and are accepted by most buyers. Check that the firm is licensed and peer-reviewed: the AICPA has publicly warned about 'quick-turn' SOC engagements.
- UK alternative: if a customer just wants 'evidence of basic security', Cyber Essentials costs £320–£600 + VAT for the self-assessment. It is not a substitute when a contract names ISO 27001.

How GRCompliance fits these numbers: ComplianceOS Community edition is free and self-hosted, which removes the platform line for teams that want to start on their own. The Audit Ready Sprint (gap assessment, policies, evidence mapping and a mock audit in 45 days) is \$14,492 in year one including the Professional licence, or \$16,892 one-time with a Lifetime licence. Your auditor's fee is billed separately by the auditor. Details at grcompliance.com/pricing.html.

7. Timelines: Type I, Type II and ISO certification

Fastest realistic path: ~3 months to a Type I, ~6-7 to a Type II

Type II requires an observation window; buyers increasingly ask for Type II specifically



Sources: Drata, Vanta (SOC 2 timelines); ISO/IEC 27006-1 & certification body guidance (ISO). Illustrative. grcompliance.com

	SOC 2 Type I	SOC 2 Type II	ISO 27001
What it proves	Controls are designed correctly at one point in time	Controls operated effectively over a period	An ISMS meets ISO 27001 and is maintained
Observation window	None	3–12 months (3 months is the practical minimum; 6–12 is common)	None, but Stage 2 expects records of the ISMS running
Typical end-to-end	1–3 months	6–12 months	4–9 months for a small, prepared company
Who issues it	Licensed CPA firm (AICPA standards)	Licensed CPA firm	Accredited certification body (e.g. UKAS-accredited)
Validity	Point in time; buyers want a fresh one yearly	Covers the period; renewed annually	3-year certificate with annual surveillance audits
Buyer acceptance	Often a stop-gap	What most US enterprise buyers ask for	Preferred in EU/UK and internationally

Sources: Drata and Vanta SOC 2 timelines (Type I 1–3 months; Type II 6–12 months; observation 3–12 months); AICPA SOC suite; ISO/IEC 27006-1 and certification-body guidance for ISO stages and the surveillance cycle.

Which one do you need?

- Selling mainly to US mid-market and enterprise: SOC 2 Type II. Start the observation window as soon as your controls are running. Consider a Type I only if a named deal will accept it.
- Selling mainly to EU/UK enterprises or internationally: ISO 27001. Many teams later add SOC 2 by mapping the same controls.
- No customer has asked yet: build the 10 public signals and core policies first (pages 15–16). The audit is easier when the habits already exist.
- A deal is blocked this month: answer the questionnaire honestly now, with gaps flagged, and give a dated plan. A credible timeline unblocks more deals than a rushed Type I.

8. The 20 questions enterprise buyers actually ask

Long questionnaires (SIG, CAIQ, custom spreadsheets) look different but ask the same core questions. We grouped the most common ones by CSA Cloud Controls Matrix domain. If you can answer these 20 with evidence, you can answer most of any questionnaire.

#	Question	CCM domain	What a good answer includes
1	Do you have a current SOC 2 Type II report or ISO 27001 certificate? Can we see it, and a bridge letter if the period has ended?	A&A	Report under NDA within a day; bridge letter ready
2	Who owns information security, and are your security policies approved and reviewed every year?	GRC	Named owner; dated, approved policy set
3	Is MFA enforced for all staff on email, code, cloud and admin consoles?	IAM	Enforced at the IdP, no exceptions
4	Do you support SAML SSO and SCIM provisioning for our users?	IAM	Yes, documented, with the plan tier stated
5	How is access granted, reviewed and removed when people leave?	IAM / HRS	Role-based access; quarterly reviews; offboarding within 24h
6	Is our data encrypted in transit and at rest? Who manages the keys?	CEK	TLS 1.2+; AES-256 at rest; cloud KMS
7	Where is our data hosted, and can you guarantee a region (e.g. EU)?	DSP	Named regions; residency options stated
8	Do you use our data to train AI models? Which AI providers receive it?	DSP / STA	Clear no-training default; AI subprocessors listed
9	Please list your subprocessors. How will you tell us about changes?	STA	Public list plus a change-notification process
10	Will you sign our DPA, or share yours (with SCCs/UK addendum)?	DSP	Standard DPA ready; redlines handled
11	How do you keep customers' data separate from each other?	IVS / AIS	Tenant isolation designed in and tested
12	Do you run an independent penetration test every year? Can we see a summary?	TVM	Annual test; executive summary and remediation status
13	How do you find and fix vulnerabilities? What are your patch deadlines?	TVM	Scanning in place; SLAs by severity (e.g. critical in 7 days)
14	Describe your secure development process: code review, dependency and secret scanning.	AIS / CCC	Required reviews; automated scanning in CI
15	What do you log, how long do you keep it, and who gets alerted?	LOG	Central logs; retention of 12 months or more; alerting
16	Do you have an incident response plan? How fast will you notify us of a breach?	SEF	Tested plan; notification within e.g. 72 hours
17	How often do you back up, and when did you last test a restore? What are your RPO and RTO?	BCR	Encrypted backups; tested restore; stated RPO/RTO
18	How are laptops secured: disk encryption, screen lock, MDM, EDR?	UEM	MDM-enforced baseline on all devices
19	Do staff get background checks, security training and sign confidentiality terms?	HRS	At hire and yearly; tracked
20	How is our data returned and deleted when the contract ends?	DSP	Export plus deletion within a stated number of days, confirmed in writing

Domains: A&A Audit & Assurance; GRC Governance, Risk & Compliance; IAM Identity & Access; HRS Human Resources; CEK Cryptography & Keys; DSP Data Security & Privacy; STA Supply Chain; IVS Infrastructure & Virtualization; AIS Application & Interface Security; TVM Threat & Vulnerability Mgmt; CCC Change Control; LOG Logging & Monitoring; SEF Incident Mgmt; BCR Business Continuity; UEM Endpoint Mgmt.
Source: CSA CCM v4 / CAIQ; Shared Assessments SIG.

How to answer when the honest answer is 'not yet'

- Never write 'yes' for a control you cannot evidence. Questionnaire answers often become contract representations.
- Use 'Partially, with a plan': describe what exists today, the gap, and a date. For example: "MFA is enforced on our IdP, GitHub and AWS. MDM rollout to all laptops completes by 30 Nov 2026."
- Keep an answer library. Buyer number five should get the same answer as buyer number one, and you should not be rewriting it each time.
- Attach evidence proactively: a policy excerpt, a pen-test summary, a screenshot of MFA enforcement. Reviewers close faster when they don't have to ask for it.

Let us answer the next one

Send us the questionnaire and what you have already (policies, past answers, trust page). We return it completed in the buyer's format, with every gap flagged honestly and a reusable answer library. Express \$750 · Standard \$1,500 · Retainer \$2,500/month. Reply to this report or visit grcompliance.com.

Common questionnaire formats

Format	Published by	Where you'll meet it
SIG Lite / SIG Core	Shared Assessments	Third-party risk teams at banks, insurers and large enterprises
CAIQ v4	Cloud Security Alliance	Cloud/SaaS vendors; mapped to the 197 CCM control objectives
HECVAT	EDUCAUSE	Higher-education buyers
Custom spreadsheet	Buyer's own	Most mid-market and enterprise buyers; often derived from SIG or CAIQ

9. 30-60-90 day readiness plan

This plan assumes a 10–50 person SaaS company on a major cloud with Google Workspace or Microsoft 365, starting from little formal documentation. It gets you to the start of a SOC 2 Type II observation window (or an ISO 27001 Stage 1 audit) in about 90 days.

Phase	What to do	Done when
Days 1–30 Foundation and visible trust	• Name a security owner and an executive sponsor • Choose your framework and scope (product, systems, people) • Build an inventory of systems, data stores and vendors • Enforce MFA everywhere; centralise accounts in your IdP • Publish: security page, security.txt, status page, subprocessor list, DPA • Draft the core policies: infosec, access control, incident response, BC/DR, vendor management, data retention • Shortlist auditors (SOC 2) or certification bodies (ISO)	Signals 1, 3–9 Found; policies drafted; scope agreed
Days 31–60 Implement and operate	• Run a risk assessment and record treatments (an ISO Statement of Applicability) • Set up onboarding/offboarding checklists and the first access review • Centralise logging and alerting; set retention • Turn on vulnerability and dependency scanning; agree patch deadlines • Roll out MDM and disk encryption; security awareness training • Back up critical data and test a restore • Assess your top vendors; collect their SOC 2 reports • Book a penetration test	Controls running and producing evidence; pen test booked
Days 61–90 Prove it	• Collect evidence against every control; fix the gaps • Run a mock audit or internal audit • Run an incident-response tabletop exercise; hold a management review • Sign the auditor; set the Type I date or start the Type II window (ISO: book Stage 1) • Publish a trust page with honest status and a report-request flow • Build your questionnaire answer library from real evidence	Audit-ready; observation window started; questionnaires answered from evidence

Shortcut: the Audit Ready Sprint runs days 1–90 of this plan in 45 days, covering gap assessment, policies, evidence mapping and a mock audit. It costs \$14,492 in year one (including the ComplianceOS Professional licence) or \$16,892 one-time with a Lifetime licence. The auditor's fee is separate. Prefer to do it yourself? Start on ComplianceOS Community, which is free, at grcompliance.com.

10. Quick wins you can ship this week

Each item below moves one of the 10 signals from Missing to Found. Together they would lift the median company in our sample from 4.5 to roughly 7 or 8, using a few days of work and almost no spend.

Action	Time	Signal	Peers missing it
Publish /.well-known/security.txt with Contact, Expires and Policy	15 min	6	79% missing
Add missing security headers in your CDN or hosting config (CSP in report-only mode first)	1–2 hrs	7	83% not Found
Set up a public status page (many tools have free tiers) and link it in the footer	1 hr	9	66% missing
Publish a subprocessor list: vendor, purpose, data location	1–2 hrs	4	72% not Found
Publish your DPA (from a reputable template, reviewed by counsel), downloadable or click-through	1 day	5	93% not Found
Write a security page: hosting, encryption, access, SDLC, testing, incident response, compliance status	Half a day	1	55% not Found
If you mention SOC 2/ISO: add the honest status, a date, and 'request the report' instructions	30 min	2	53% not Found
Document SSO (SAML/OIDC) and MFA support on your pricing or docs page	30 min	8	77% not Found
Configure your consent tool so trackers wait for opt-in; remove tags you don't use	2 hrs	10	25% missing
Enforce MFA for all staff on your IdP, GitHub and cloud console (internal, but always asked)	1 hr	—	Question 3 on p.13

References: RFC 9116 (security.txt); OWASP Secure Headers Project; GDPR Art. 28 (processor obligations, sub-processors).

Copy-paste starter: security.txt

Contact: <mailto:security@yourcompany.com>
 Expires: 2027-10-14T00:00:00Z
 Policy: <https://yourcompany.com/security#disclosure>
 Preferred-Languages: en

Serve it at <https://yourcompany.com/.well-known/security.txt> as text/plain. Update Expires at least once a year (RFC 9116 recommends less than a year ahead).

Not sure which of these you already have?

Ask for a free Readiness Snapshot. We run all 10 checks on your domain and send a one-page result with your score and top 5 fixes. It is passive, uses public information only, and needs no access. Reply to this report or visit grcompliance.com.

11. One-page self-assessment

Print this page or copy it into a doc. For each signal, check your public site as a buyer would: logged out, in a private browser window. Tick one box per row.

#	Signal	Pass if...	Found (1)	Partial (0.5)	Missing (0)
1	Security / trust page	A page with real content (encryption, access, testing, incident response), linked from the footer	☐	☐	☐
2	SOC 2 / ISO evidence path	Honest status plus a way to obtain the report or certificate (trust centre or request flow)	☐	☐	☐
3	Privacy policy	Current, specific, names the controller and contact	☐	☐	☐
4	Subprocessor list	Public, with vendor, purpose and location; change-notice process	☐	☐	☐
5	DPA	Downloadable or click-through; SCCs/UK addendum referenced	☐	☐	☐
6	security.txt	/.well-known/security.txt returns text/plain with Contact and Expires	☐	☐	☐
7	Security headers	5+ of: HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy (check with your browser dev tools or a header checker)	☐	☐	☐
8	SSO / MFA	SAML/OIDC SSO and MFA support stated publicly	☐	☐	☐
9	Status page	Public, linked, shows incident history	☐	☐	☐
10	Cookie consent	Trackers wait for consent, or there are no trackers	☐	☐	☐

0–4 Early

Start with the quick wins on page 16. Expect questionnaires to stall deals.

4.5–7 Developing

Close the legal gaps (DPA, subprocessors) and publish a trust page. Plan your audit.

7.5–10 Advanced

Ahead of 87% of peers. Keep it current and make the reports easy to request.

My score: _____ / 10 **Peer median:** 4.5 **Date checked:** _____

Want a second pair of eyes? Send us your domain and we will run the same check and send back a scored Readiness Snapshot, free.

12. Method and limitations

Sample

We reviewed 132 company websites and scored 130 (2 could not be loaded reliably). The companies came from three public sources: startups whose pre-seed to Series B funding was announced in roughly August–October 2026 (from public funding news and our research lists); companies publicly hiring for security, GRC or SOC 2 roles, or publicly stating that SOC 2 is in progress (from job posts and trust pages); and 19 more recently funded companies from public press coverage (tech.eu, TechCrunch, PR Newswire, MobiHealthNews and company press pages) that we added to widen the sample. Duplicates across sources were merged. GRC and compliance-software vendors found in press coverage were excluded so we would not be benchmarking our own competitors.

What we checked (passive only)

- One normal request to each homepage (headers and HTML), plus a headless-browser render so we could see JavaScript-loaded content and consent banners.
- Up to 10 well-known public paths (for example /security, /trust, /privacy, /legal/subprocessors, /dpa, /.well-known/security.txt), each compared with a random non-existent path to filter out 'soft 404' pages.
- Public DNS lookups (DNS-over-HTTPS) for trust., status. and security. subdomains, and up to 9 linked public pages such as trust centres, status pages and legal pages.
- No port scanning, vulnerability scanning, logins, form submissions or contact with any company. Data was collected on 14 October 2026.

Scoring and validation

Each signal was scored Found, Partial or Missing by documented rules (for example, headers are Found with HSTS plus at least 5 of 6 headers). For 17 companies we had already done a full manual review, and for these we used the manual result. Comparing the automated rules with the manual review on those 17 companies, the two agreed on 144 of 170 signal judgements (85%). Where they disagreed, the rules were usually stricter, scoring Missing where a person scored Partial. So the overall scores here are, if anything, slightly conservative.

Limitations: please read before quoting

- Public signals are not security. A company can be well run and show nothing publicly, or the opposite. This is a measure of visible, buyer-grade evidence only.
- We undercount anything behind a login, NDA or email request: private trust portals, DPAs sent on request, reports shared in a deal room.
- We did not verify any SOC 2 or ISO claim. 'Mentions SOC 2' means the text appears on public pages, which may include 'in progress'.
- The sample is not random. It is skewed toward recently funded companies in our research lists and toward AI-related startups, which matches the 2026 funding market. The hiring and 'in progress' groups are small (7–8 companies each) and self-selected.
- Sector and region come from public descriptions and legal-entity text and are approximate. 23 companies' region could not be determined and are shown as Unknown.
- Consent banners that appear only after interaction or a delay may have been missed, and trackers were checked on the homepage only.
- A single snapshot in time. Websites change weekly.

Anonymity

No company is named in this report. All figures are aggregated, and segments with fewer than 4 companies are not shown separately. We will not disclose company-level results from this study. Any company that wants its own result can request a private Readiness Snapshot.

13. Sources and about GRCompliance

- [1] AICPA & CIMA — SOC suite of services, and notice on quick-turn SOC engagements (2026) <https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2>
- [2] Drata — How Much Does a SOC 2 Audit Cost? (2026) <https://drata.com/learn/soc-2/cost>
- [3] Vanta — How much does a SOC 2 audit cost? <https://www.vanta.com/collection/soc-2/soc-2-audit-cost>
- [4] iso27001partners.co.uk — ISO 27001 certification cost UK (reproduces ISO/IEC 27006-1:2024 Table C.1; reviewed Oct 2026) <https://iso27001partners.co.uk/iso-27001-certification-cost/>
- [5] Blaze Information Security — Penetration Testing Cost & Pricing 2026 <https://www.blazeinfosec.com/post/how-much-does-penetration-testing-cost>
- [6] Cloud Security Alliance — Cloud Controls Matrix and CAIQ v4 <https://cloudsecurityalliance.org/research/cloud-controls-matrix>
- [7] Shared Assessments — Standardized Information Gathering (SIG) questionnaire <https://sharedassessments.org/sig/>
- [8] IETF RFC 9116 — A File Format to Aid in Security Vulnerability Disclosure (security.txt) <https://www.rfc-editor.org/rfc/rfc9116>
- [9] OWASP Secure Headers Project <https://owasp.org/www-project-secure-headers/>
- [10] GDPR Article 28 — Processor <https://gdpr-info.eu/art-28-gdpr/>
- [11] GRCompliance pricing (ComplianceOS, Audit Ready Sprint, Questionnaire Service) <https://grcompliance.com/pricing.html>

About GRCompliance

GRCompliance builds ComplianceOS, an open-core GRC platform for SOC 2, ISO 27001, HIPAA, GDPR and NIST. It is self-hosted with unlimited users, and the Community edition is free. For teams that need help faster, we offer fixed-scope services:

Offer	Price	What you get
Readiness Snapshot	Free	One-page public-signal score with your top 5 gaps
ComplianceOS Community	Free	Open-core, self-hosted GRC platform. Start building policies and controls today
Security Questionnaire Service	\$750 Express · \$1,500 Standard · \$2,500/mo Retainer	SIG Lite, CAIQ and custom questionnaires completed honestly, at a fixed price
Audit Ready Sprint	\$14,492 year 1 (incl. Professional licence) · \$16,892 with Lifetime licence	Gap assessment, policies, evidence mapping and mock audit in 45 days. Auditor fees are billed separately by the auditor

Get your free Readiness Snapshot

Request yours at app.grcompliance.com/waitlist, or visit grcompliance.com. For pricing, see grcompliance.com/pricing.html.

Dante Wells · GRCompliance · grcompliance.com

© 2026 GRCompliance. Free to share with attribution. This report is general information, not legal or audit advice. Vendor price ranges are as published by the cited sources in 2026 and may change.