

Raize Orion Compliance

Ten compliance frameworks. One source of truth.

AI-assisted, multi-framework GRC built for SaaS scale-ups.

10

Frameworks supported

19

Evidence connectors

1,600+

Pre-mapped controls

99.5%

Uptime SLA

Raize Orion Compliance is a multi-framework GRC platform for SaaS scale-ups. One workspace for ISO 27001, SOC 2, NIST 800-53, GDPR, HIPAA, PCI DSS, ISO 22301, NIS2, Cyber Essentials and IASME Cyber Assurance - with automated evidence collection from 19 cloud, identity and observability sources, AI-assisted policy authoring, a public Trust Center, and an auditor portal that does not fight you. Built UK-side with EU data residency.

Who this is for

- SaaS companies in the 10-500 employee band entering or maintaining a compliance programme
- Compliance consultants needing a multi-tenant tool to operate audits across clients
- In-house security leads who want to demonstrate continuous compliance to customers + the board
- Buyers replacing Vanta or Drata to consolidate cost or to add HIPAA / PCI DSS / NIST 800-53 coverage

Book a 30-minute demo

sales@raizehq.dev - +44 7350 160740 - raizehq.dev

Why teams choose Raize Orion

Most GRC tools force you to pick a single framework, then pay-per-add. Raize Orion ships ten frameworks cross-mapped at the control level so a single piece of evidence satisfies every framework it touches. Add EU data residency, AI-assisted authoring, and sales-led pricing that scales with team shape rather than seat count, and the build-vs-buy maths flips.

Six things that matter to buyers

Multi-framework, cross-mapped

Every control is pre-mapped across ISO 27001 Annex A, SOC 2 TSC, NIST 800-53, HIPAA Security Rule, PCI DSS v4.0.1, GDPR / UK GDPR articles, ISO 22301 clauses 4-10, NIS2 Art. 21 measures, Cyber Essentials themes, and IASME Cyber Assurance themes. Adopt a policy once, satisfy every framework that touches it.

Automated evidence collection

19 connectors (AWS, GCP, Azure AD, GitHub, Okta, Auth0, Google Workspace, ServiceNow, CrowdStrike, Snowflake, Slack, Datadog, Jira, Cloudflare, Sentry, BambooHR, Jamf, Kandji, plus a generic REST/JSON connector for in-house systems) pull control evidence on a daily cron, written into a tamper-evident audit log.

AI-assisted policy authoring

Generate first-draft policies (Information Security, Acceptable Use, Incident Response, etc.) tuned to your industry + risk profile. Edit + adopt + version-control.

Public Trust Center + Auditor Portal

Bundled at base tier. Share scope-bounded read-only links with prospects + external auditors without an NDA negotiation. Customer self-service evidence in days, not weeks.

EU data residency + UK incorporation

All customer data hosted in EU-West-1 (AWS Frankfurt). Processor under UK GDPR. Real wedge vs US-built tools when winning EU + FS deals.

Realtime drift alerts to Slack

Connector findings at or above your configured severity threshold post to your Slack channel within seconds - the "Compliance OS" pattern, not a once-a-day digest.

Frameworks supported

Ten frameworks shipped first-class, with framework allowances scaling per plan (3 / 6 / all 10). Cross-mapped at control level so each piece of evidence satisfies every framework it touches.

ISO 27001:2022

International (ISO/IEC) - 93 Annex A controls + 22 management clauses

Use case: EU customers; tender requirement; ISMS certification path.

SOC 2 (TSC 2017)

AICPA - CC1-CC9 + A1 + C1 + PI1 + P1 (201 criteria)

Use case: US enterprise customers; vendor security assessments.

NIST 800-53 Rev 5

US Federal - ~1,061 controls across 20 control families

Use case: US federal contracting; FedRAMP path; depth + rigour benchmark.

GDPR / UK GDPR

EU + UK Regulation - 50 article-mapped controls + DPIA + RoPA + DSR

Use case: Any EU customer data; processor + controller workflows.

HIPAA

US Federal (Healthcare) - 52 sec. 164 specifications + BAA workflow

Use case: Healthcare customers; BAA-required vendors.

PCI DSS v4.0.1

PCI SSC - 52 controls across 12 requirements + Req. Tab

Use case: Payment-card-handling customers; merchant + service-provider variants.

ISO 22301:2019

International (BCMS) - 37 requirements across clauses 4-10 + BIA + RTO/RPO

Use case: Business continuity; tender requirement; supply-chain assurance.

NIS2 ((EU) 2022/2555)

EU Directive - 32 reqs - Art 21 ten measures + Art 23 reporting clock

Use case: EU essential / important entities; 24h / 72h / 1-month reporting.

Cyber Essentials / Plus

UK Government - 40 controls across five technical themes + CE Plus verification

Use case: UK public-sector contracts; baseline UK cybersecurity hygiene.

IASME Cyber Assurance

UK Standard (risk-based) - 61 requirements across 13 themes (incl. Cyber Essentials)

Use case: UK SMEs; risk-based assurance + GDPR + business continuity bundled.

Evidence connectors

19 connectors auto-collect compliance evidence on a daily cron. Findings tagged to the framework controls they satisfy (ISO 27001 / SOC 2 / NIST 800-53 / HIPAA / PCI / GDPR / ISO 22301 / NIS2 / CE / IASME), framework-gated against your active programmes.

Connector catalogue (19)

Source	What we evidence	Control codes (sample)
AWS	IAM users + MFA, S3, KMS, CloudTrail	CC6.1, CC6.8, A.5.16, A.5.18
GCP	IAM, service-accounts, KMS keys, audit logs	CC6.1, A.5.15, AU-2
Azure AD	Conditional access, privileged roles	CC6.1, A.5.18, AC-2(7)
Okta	Password policy, MFA enrolment, admins	CC6.2, IA-2(1), A.5.17
Auth0	Tenant settings, MFA, rule inventory	CC6.2, A.5.17, IA-2
Google Workspace	2-step verification %, super-admins	CC6.2, IA-2(1), 164.312(d)
GitHub	Branch protection, MFA, Dependabot	CC8.1, A.5.17, AC-2
ServiceNow	Change-request volume, incident age	CC8.1, CC7.4, A.5.26, IR-4
CrowdStrike	Endpoint coverage %, agent versions	CC6.8, A.8.7, SI-3
Snowflake	Network policies, MFA %, dormant users	CC6.2, CC6.6, IA-2(1), SC-7
BambooHR	Joiner / mover / leaver lifecycle	CC1.4, A.6.1, PS-4
Jamf	macOS fleet posture (disk encrypt., patches)	A.8.7, A.8.8, SI-2
Kandji	macOS fleet posture (zero-touch, MDM)	A.8.7, A.8.8, SI-2
Slack	2FA scope, workspace reachability	CC6.2, A.5.17
Datadog	Monitors, log retention, alerts, SLOs	CC7.1, CC7.2, AU-11, A.8.15
Jira Cloud	Auth + project inventory	CC8.1, A.5.16
Cloudflare	API-token scope, zone inventory	CC6.1, A.5.16
Sentry	Project inventory, error retention	CC7.3, A.5.25
Generic REST/JSON	Custom in-house source mapped to control codes	Any (declared per connector)

Framework-gated deep checks + realtime drift alerts

Each connector runs framework-gated deep checks based on your organisation's enabled frameworks - so a PCI-only org sees PCI-relevant findings, not noise. A control-code relevance guard ensures evidence is only mapped to controls that exist in your active catalogues. Configure a Slack webhook + severity threshold per organisation: findings at or above the threshold post to your channel within seconds, with control codes + a deep-link back to the evidence record. Included at every plan tier.

Feature matrix

Programme management

- Multi-framework control library (1,600+ pre-mapped)
- Custom controls + per-tenant overlays
- Cross-framework control mapping
- Maturity model (CMMI-aligned)
- Statement of Applicability (SoA)

Evidence + automation

- 19 evidence connectors (daily auto-collect)
- Framework-gated deep checks + relevance guard
- AI evidence scoring + relevance match
- Manual evidence upload + tagging
- Realtime drift alerts to Slack

Policy + AI

- 52 policy templates (multi-framework)
- AI-assisted policy authoring + revision
- Policy versioning + adoption workflow
- AI policy gap analysis
- Per-org branded DOCX export

Risk + DPIA + ROPA

- Risk register with CVSS-aligned likelihood x impact
- Risk treatment + KRI tracking
- DPIA module (GDPR Art. 35)
- ROPA module (GDPR Art. 30)
- Vendor risk assessments + questionnaires

Audit + reporting

- Internal audit + AOC findings + CAPA
- Auditor portal (scope-bounded tokens)
- Audit log export (CSV) - lifetime + 30d retention
- Board pack PDF generator
- Per-framework attestation reports

Trust + sales support

- Public Trust Center per organisation
- Customer-facing questionnaire response library
- CAIQ v4 + SIG Lite 2024 + HIPAA BAA templates
- Sub-processor disclosure + change notifications
- Status page (commits to RTO 4h / RPO 1h / uptime 99.5%)

Plans

Three plans sized for different team shapes. Auditor Portal, Trust Center, audit log and the full evidence-connector catalogue are available across plans. Pricing is sales-led - email sales@raizehq.dev for a same-day quote tailored to framework scope, rollout timing and team size.

Starter

Pick 3 frameworks, small team.

- 3 frameworks (your choice)
- 5 users
- 1 evidence connector
- Auditor portal + Trust Center
- Custom controls

Growth (most popular)

Full GRC stack + AI.

- 6 frameworks (your choice)
- 25 users
- All 19 evidence connectors
- AI scoring + policy + chat
- Up to 5 webhook endpoints
- Priority support

Enterprise

All frameworks + dedicated CSM.

- All 10 frameworks
- Unlimited users + AI
- SCIM provisioning (Okta, Azure AD)
- Annual billing options
- Custom DPA on request
- Dedicated CSM + SLA

For a quote sized to your team and framework scope, email sales@raizehq.dev or call +44 7350 160740. Billing is GBP-default with USD (\$) and EUR (€) on request. No long-term commitment - cancel any time from the in-app Customer Portal.

Security + compliance posture

Our own commitments

Commitment	Value
Uptime SLA	99.5% (rolling 30d)
RTO (Recovery Time Objective)	4 hours
RPO (Recovery Point Objective)	1 hour
P1 incident acknowledgement	30 minutes
Customer breach notification	Within 72 hours (UK GDPR Art. 33)
Audit log retention	Lifetime of contract + 30 days + 7y off-site
Customer data deletion (on request)	Within 30 days + deletion certificate
Data residency	EU-West-1 (AWS Frankfurt)
Encryption at rest	AES-256
Encryption in transit	TLS 1.2+ (1.3 preferred); HSTS preload
MFA enforcement	Mandatory on every user role

Compliance status

Raize Technologies Ltd holds a complete day-1 SOC 2 Type II evidence pack (17/18 items prepared; DBS check + pen test in flight). Type I targeted Q3 2026, Type II report Q1 2027. ISO 27001 readiness package complete; certification body engagement scheduled. UK GDPR + DPA in force at <https://raizehq.dev/dpa>.

Sub-processors

- Supabase (Postgres + Auth + Storage + Vault + Edge Functions) - EU-West-1
- Vercel (CDN + edge runtime) - EU regions
- Stripe (billing) - EU + global, PCI Level 1
- Resend (transactional email) - US/EU
- Anthropic (AI features - policy authoring, scoring, chat) - US, DPA signed
- Voyage AI (embeddings for evidence semantic search) - US, DPA signed
- Sentry (error monitoring) - EU region
- Cloudflare (DNS only) - global
- GitHub (source control) - US

Full sub-processor disclosure + change notifications: raizehq.dev/trust/raize. 30-day advance notification on material changes.

How Raize compares + onboarding

vs Vanta / Drata at a glance

Capability	Raize Orion	Vanta	Drata
Frameworks shipped first-class	10	6 + add-ons	6 + add-ons
HIPAA + PCI DSS bundled	Yes	Add-on	Add-on
NIS2 + ISO 22301 + CE + IASME	Yes	No	No
Public Trust Center	Bundled	Bundled	Add-on
Realtime drift alerts	Yes	Yes	Yes
EU data residency	Native	US (GDPR opt-in)	US (GDPR opt-in)
AI policy authoring	Bundled	Add-on	In beta
Sales-led pricing + UK-based team	Yes	No	No

Onboarding - what to expect

- Day 0** Book a 30-minute demo at sales@raizehq.dev or +44 7350 160740; choose 3 (Starter), 6 (Growth) or all 10 (Enterprise) frameworks.
- Day 1** Walk through the per-framework gap analysis - pre-populated with the controls likely already covered by your current stack. Connect first evidence source (typically Okta or GitHub) in under 10 minutes.
- Day 3** Adopt baseline policies (Info Sec, AUP, IR, BCP, Vendor Risk, etc.) from the 52-template library via the AI-assisted authoring flow. Edit, route through your approver, mark adopted.
- Week 1** Populate Risk + Vendor + Asset registers; seed the audit log; configure the Trust Center for your prospects to consume.
- Week 2** Schedule your first auditor portal share; commission a pen test if you do not already have one; book the kick-off with your chosen audit firm.
- Month 2** Cron-driven evidence rolls in daily across all 19 connectors; Slack alerts surface drift; quarterly synthetic audits keep the programme honest.

Ready to start?

Sales: sales@raizehq.dev - +44 7350 160740
 Support: support@raizehq.dev - response within 1 business day
 Privacy: privacy@raizehq.dev - DSR fulfilment within 30 days