COMPLIANCE PACKS · DATASHEET

Safeguard

One body of evidence for ISO 27001, HIPAA, GDPR, PCI DSS and NIST.

Choose the frameworks that apply, connect your systems once, and let the same evidence answer more than one standard.

THE PROBLEM

Each framework arrives with its own spreadsheet, its own owner and its own audit calendar, and the same access review gets collected three times. Teams that work under more than one standard spend their effort on duplicate evidence, not on closing gaps.

WHAT IT DOES

The frameworks you need

ISO 27001, HIPAA, GDPR, PCI DSS and NIST are in the library, alongside SOC 2 and many more. Switch on the ones that apply to you.

Automated tests

Connected systems run tests that map to the controls of SOC 2, ISO 27001, the HIPAA Security Rule, PCI DSS and NIST CSF 2.0.

Evidence reused

A crosswalk carries that evidence to equivalent controls of related frameworks, including NIST SP 800–53, so you collect it once.

Policies and attestations

Every framework has policy templates to start from, and a requirement a scan cannot see passes when a person attests it with evidence.

HOW IT WORKS

1. **Choose** — Switch on your frameworks
2. **Connect** — Cloud, identity and code systems
3. **Test** — Automated tests map to controls
4. **Attest** — People attest what a scan cannot see
5. **Report** — Readiness by framework

A READINESS SCORE IS NOT AN AUDIT OPINION

It is Safeguard's assessment of what it can see, and it shows how many requirements a scan evaluated and how many need evidence. Choosing a framework does not certify compliance.

CAPABILITIES IN DETAIL

Frameworks	ISO/IEC 27001, the HIPAA Security Rule, GDPR, PCI DSS and the NIST family, including CSF 2.0 and SP 800-53, each with its own page in the docs.
Scan requirements	Checked on each scan of a product, including its software inventory. Each requirement is decided by a scan or needs evidence.
Automated tests	Map directly to SOC 2, ISO 27001, HIPAA Security Rule, PCI DSS and NIST CSF 2.0, and to the CIS benchmarks.
GDPR	Covered by scan requirements, controls, policy templates and your own evidence.
Controls	Linked to tests, policies and uploaded evidence. Custom controls are supported.
Readiness	The share of in-scope requirements that pass. A requirement can be scoped out with a written justification.
Trust Center	Publish your posture and documents, and control who can see them.

INPUTS

- The frameworks you choose
- Connector sign-in for cloud, identity and code systems
- Uploaded evidence and policies
- Attestations from named people

OUTPUTS

- Readiness by framework
- Evidence mapped to controls
- Policy drafts
- Tasks for gaps
- Reports for your auditor

INTEGRATIONS AND SURFACES

Google Workspace · Google Cloud · Cloudflare · GitLab · Jira · CIS benchmarks · Trust Center · Policy templates

DEPLOYMENT AND DATA HANDLING

Regions and hosting
SaaS in US, EU (Frankfurt) and Gov regions. Private VPC, on-prem and fully air-gapped deployments are available.

Model choice
Zero AI mode runs the platform deterministically with no LLM. Or bring your own model (Claude, OpenAI and others), or run Safeguard models inside your environment.

Evidence handling
Evidence is tenant scoped, and the connector sign-in you grant controls what Safeguard can read.

Access control
SSO (SAML 2.0, OpenID, Google, Microsoft, GitHub), roles and 2FA.

Safeguard helps you produce evidence and map controls. It does not make an organization compliant by itself.

Browse the framework library

safeguard.sh/frameworks

Scan the code or type the address. Questions: hi@safeguard.sh

Safeguard

SOC 2 Type I and Type II audited; reports available on request (safeguard.sh/trust). Designed for FedRAMP High.