ControlSage

The SAGE Framework

Frictionless compliance, managed within the tools you already trust.

Published by ControlSage

Our Value

The principles that guide everything we do.

S — Strategize

We design a clear audit roadmap that works perfectly with your existing tools.

A — Align

We map your specific security controls to strict industry standards without adding software.

G — Govern

Our experts manage your daily compliance needs directly inside your chosen software platforms.

E — Evolve

We scale your security program over time to ensure permanent and complete readiness.

Table of Contents

1. Why SAGE Exists

The default way most companies get compliant is to buy a new platform, migrate their evidence into it, and ask their team to learn a new tool on top of everything they already use. That approach solves the compliance problem by creating a second one: software sprawl, a new system nobody outside the security function logs into, and evidence that lives somewhere disconnected from the engineering, IT, and operational workflows that actually produce it.

SAGE starts from a different premise: **the tools you already use — your ticketing system, your identity provider, your existing GRC platform if you have one, your spreadsheets if you don't — are usually sufficient.** What's missing isn't more software. It's a clear roadmap, disciplined control mapping, consistent daily management, and a plan to scale — delivered by people who work inside the systems you already trust, rather than asking you to adopt theirs.

That's the whole framework: **Strategize, Align, Govern, Evolve.** Four phases, no new platform, one accountable partner managing the work inside your existing stack.

> *In Practice: If you're already running evidence through AuditBoard, Archer, ServiceNow, or even a well-organized set of shared drives and spreadsheets, SAGE is designed to work inside that — not replace it.*

2. The SAGE Framework at a Glance

Phase	Core question it answers	Primary output	Typical cadence
Strategize	What do we actually need, and in what order?	An audit roadmap scoped to your real requirements and existing tools	Weeks 1–2
Align	Do our controls actually satisfy the standards we're targeting?	A control-to-framework crosswalk and gap analysis	Weeks 2–5
Govern	Who's keeping this running day to day?	Ongoing evidence management inside your existing platforms	Continuous, monthly cadence
Evolve	How does this hold up as we grow?	A living roadmap that expands with headcount, frameworks, and regions	Quarterly review

Each phase produces the input the next phase needs — Strategize sets the scope Align maps against, Align produces the control library Govern maintains, and Govern produces the evidence trail Evolve builds on when it's time to scale. Nothing is thrown away and rebuilt between phases.

3. S — Strategize

We design a clear audit roadmap that works perfectly with your existing tools.

Every engagement starts here, because the single most expensive mistake in compliance is scoping the wrong thing — pursuing a framework nobody's asking for, or scoping in criteria that add audit burden without adding sales value.

What happens in this phase

- A scoping session covering your customer base, deal pipeline, data sensitivity, and any specific framework requests already in hand
- An inventory of your existing tooling — identity provider, cloud infrastructure, ticketing system, any GRC platform already in place — so the roadmap is built around what you have, not around a hypothetical clean slate
- Framework selection and Trust Service Criteria (or equivalent) scoping, informed by which frameworks are already covered in the Choosing Your First Framework crosswalk
- A written roadmap with milestones, target audit dates, and a clear owner for each workstream

What you get

A roadmap document your team, your investors, and your auditor can all read and agree on — before any control work begins.

4. A — Align

We map your specific security controls to strict industry standards without adding software.

Alignment is where the roadmap becomes a control library. This is deliberately the most detail-heavy phase, because a rushed control mapping is what produces failed audits and re-work later.

What happens in this phase

- Every control the roadmap identified gets mapped against the specific clauses of your target framework (SOC 2 Trust Service Criteria, ISO 27001 Annex A, HIPAA safeguards, PCI DSS requirements, GDPR articles, or NIST controls)
- A gap analysis identifies which controls already exist and operate correctly, which exist but need tightening, and which don't exist yet
- Where multiple frameworks are in scope, controls are mapped once against a unified library — not duplicated per framework — so the work compounds instead of repeating
- All of this happens inside the tools you already use to track work: your ticketing system for remediation items, your existing document store for policies, your existing GRC platform for evidence if you have one

What you get

A control-to-framework crosswalk and a prioritized remediation list, with no new software to provision or migrate data into.

5. G — Govern

Our experts manage your daily compliance needs directly inside your chosen software platforms.

This is the phase where most external compliance help disappears, leaving the internal team to run evidence collection alone until the next audit. SAGE treats governance as an ongoing managed function, not a handoff.

Recurring Evidence Collection

Access reviews, vulnerability scan follow-ups, policy acknowledgment tracking, vendor register updates — run on a defined cadence inside your existing systems.

Named Point of Contact

A dedicated owner for evidence completeness, so it isn't diffused across your team the way unowned compliance work usually is.

Direct Platform Engagement

Pulling evidence from your identity provider and cloud accounts, logging remediation in your existing ticketing system — not asking your engineers to log into a separate compliance tool.

Continuous Readiness

When audit season arrives, evidence collection is a formality rather than a scramble.

What you get: a compliance function that runs itself between audits, without requiring your team to adopt new daily habits or new software.

6. E — Evolve

We scale your security program over time to ensure permanent and complete readiness.

The Evolve phase is what keeps a program from becoming the "rebuild trap" — the point where growth, new frameworks, or new regions would otherwise force a from-scratch restart.

What happens in this phase

- Quarterly reviews of the program against company growth: new headcount, new products, new customer segments, new regions
- Proactive framework expansion planning — identifying when a second or third framework (ISO 27001, HIPAA, PCI DSS, GDPR, NIST) is likely to become necessary, before it becomes urgent
- Maturity progression — moving the program from simply passing audits toward board-level reporting, risk reduction, and M&A readiness
- Ongoing tooling recommendations as your team and infrastructure grow, still evaluated against the same principle: extend what you have before adding something new

What you get

A program that gets easier to maintain and faster to audit each year, instead of one that quietly falls out of date the moment the initial engagement ends.

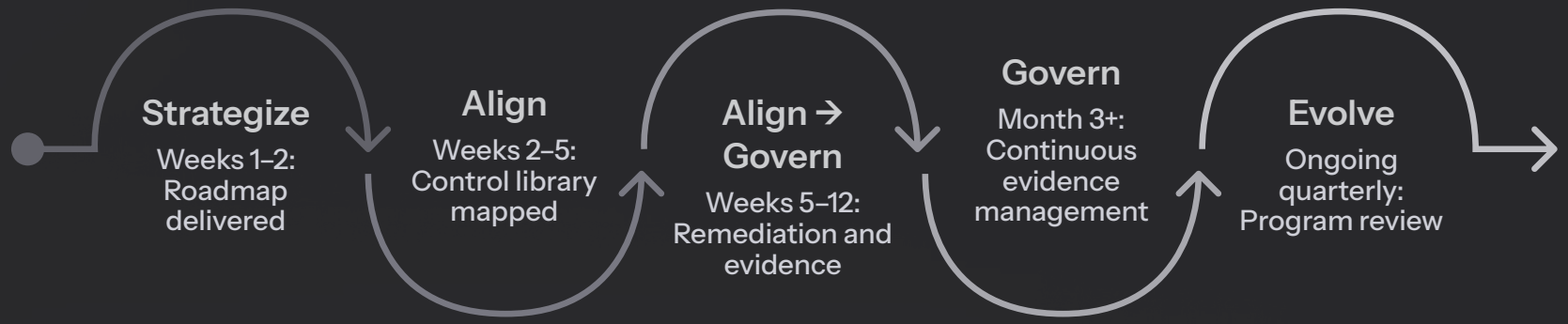
7. Why "No New Software" Matters

Every SAGE phase repeats the same constraint deliberately: work inside the tools you already trust. This isn't a cost-cutting shortcut — it's a structural choice with real downstream effects.

Traditional approach	SAGE approach
Buy a GRC platform, migrate evidence into it	Work inside your existing systems — GRC platform, spreadsheets, or ticketing tools
Team learns a new tool to participate in compliance	Compliance happens inside tools your team already uses daily
Evidence lives in a system disconnected from where work happens	Evidence is pulled from the systems that actually produce it
Compliance ownership concentrated in one platform's admin	Ownership distributed across the same roles already responsible for the work
Switching vendors means a full data migration	Switching or expanding is additive, not a migration project

The result is lower total cost — not just in software licensing, but in the adoption friction that quietly kills most compliance initiatives before they produce a usable evidence trail.

8. The SAGE Journey



Timeframe	Phase	Milestone
Weeks 1–2	Strategize	Roadmap delivered and agreed with your team
Weeks 2–5	Align	Control library mapped, gap analysis complete
Weeks 5–12	Align → Govern	Remediation of identified gaps, evidence collection begins
Month 3 onward	Govern	Continuous evidence management, audit-ready posture maintained
Ongoing, quarterly	Evolve	Program reviewed and adjusted for growth, new frameworks, new regions

Strategize and Align are front-loaded, intensive phases. Govern and Evolve are the permanent, lower-effort steady state the first two phases are designed to produce.

9. Who SAGE Is Built For

SAGE is designed to meet companies wherever they are in the compliance journey:

Companies without a foundation yet

Start in Strategize and Align, building the core control layer described in *Build Security Into Your Foundation*.

Companies with one framework, expanding to more

Use Align's unified control library to avoid the rebuild trap described in *Startups Move Fast, Security Should Scale*.

Companies past their first audit, looking to optimize

Move quickly through Strategize and Align and spend most of their time in Govern and Evolve, working toward the board-level maturity described in *Built for Companies Ready for What's Next*.

In every case, the constraint stays the same: the work happens inside the tools you already trust.

10. Frequently Asked Questions

Do we need to buy new software to work with SAGE?

No. SAGE is explicitly designed to work inside your existing identity provider, cloud accounts, ticketing system, document store, and GRC platform if you already have one. If a genuine tooling gap exists, we'll recommend closing it — but that's the exception, not the starting assumption.

How much time does our team need to commit?

Most heavily during Strategize and Align, where scoping sessions and control mapping need input from engineering and leadership. Once Govern begins, ongoing time commitment from your team drops significantly, since evidence collection is managed on your behalf inside your existing systems.

What if we're already mid-way through a compliance effort?

SAGE can start at Align or Govern rather than from scratch — the framework is designed to pick up wherever your current program actually is, not to assume a blank slate.

Does SAGE work across multiple frameworks at once?

Yes — this is where the Align phase's unified control library matters most. A single control mapped once can satisfy SOC 2, ISO 27001, HIPAA, PCI DSS, GDPR, and NIST simultaneously, rather than being re-mapped per framework.

11. Closing Note

> SAGE isn't a platform you adopt — it's a way of working that assumes the platforms you already have are enough, if the strategy, mapping, daily management, and growth planning around them are handled well.

1. **Strategize**
   Sets the direction
2. **Align**
   Proves your controls hold up
3. **Govern**
   Keeps it running without changing how your team works
4. **Evolve**
   Ensures nothing has to be rebuilt when you grow

ControlSage runs the SAGE Framework for startups and scaling companies who want compliance handled — inside the tools they already trust, not a new one they have to learn.