intSignal Research & Compliance

SOC 2 · ISO 27001 · HIPAA

Compliance Program Handbook & Evidence Workbook

One complete source for planning, running, and evidencing your compliance program — with instructions, guidance, and fillable forms for every control domain, for teams of any size.

Run this program free at portal.intsignal.com/compliance

v1.0 · September 2026

Table of contents

PART 1

Foundations

Before the controls: how to use this handbook, what auditors actually test, which framework to work, how to run the program, and how to scale it to your size.

1.1 How to use this handbook

This is a complete, standalone reference. You can work it on paper, but it pairs with the free **intSignal Compliance Workspace**, which turns every form here into a fillable control with an evidence vault, live readiness scoring, tasks, and a one-click auditor export.

Work it in three passes. **First**, read Choosing your framework (p. 3) and pick one. **Second**, walk the control domains (p. 5) in Part 2 — for each, read the guidance, then fill the forms and gather the evidence. **Third**, use the master evidence index (p. 16) to track what's done and export your auditor pack (p. 17).

LITE / SMALL COMPANY

A small company can run the whole program from this handbook plus the free workspace, with one owner and a weekly hour. Start with the fundamentals — access, MFA, encryption, backups, and policies — and skip nothing, but keep the forms lightweight.

ENTERPRISE / HEAVY USE

Larger organizations should assign a domain owner per Part 2 section, run the forms as living registers (in the workspace or your GRC tool), and hold a recurring review. The same structure scales — you're adding owners and cadence, not new steps.

1.2 What compliance evidence is

Auditors test two things about every control: that it is **designed** (you have a way to do it) and that it is **operating** (you actually do it, over time). Evidence has to show both.

Good evidence falls into four types: **policies** (the written document), **configurations** (a screenshot or export showing a setting is enforced), **records of operation** (a completed review, a resolved incident — proof the process ran, with a date), and **tickets and logs** (system-generated, hard to fake, easy to date).

TIP

Favor dated, system-generated evidence over hand-made documents. An access review exported from your identity provider beats a screenshot pasted into a doc — it's more credible and far easier to refresh next year.

1.3 Choosing your framework

All three share the same security fundamentals; the differences are in emphasis and audience.

Framework	What it is	Choose it when
SOC 2	A CPA attestation against the Trust Services Criteria (security required; availability, confidentiality, processing integrity, privacy optional). Type II tests operation over a period.	Customers and prospects ask for a security report during procurement (most B2B SaaS).
ISO 27001	International certification that you run an ISMS and applied the relevant Annex A controls, with a Statement of Applicability.	You sell internationally, or a buyer named the standard.
HIPAA	US regulation (not a certificate) for anyone handling PHI — administrative, physical, and technical safeguards plus privacy duties.	You create, receive, maintain, or transmit protected health information.

TIP

These overlap heavily — access control, encryption, logging, incident response, and vendor management appear in all three. Evidence you gather for one usually satisfies the others, so a second framework later is far less than double the work.

1.4 Running the program

Work every control the same way, in passes rather than perfecting one at a time.

Set a status for each control — *not started*, *in progress*, *implemented*, or *N/A* with a justification. **Add notes** describing how you meet it, for an auditor who has never seen your environment. **Attach evidence** that proves it. **Assign an owner and due date** so the work is shared, and let reminders keep it moving.

The three passes: **(1) triage** — set every control's status so your readiness score and gap list reflect reality; **(2) easy wins** — close controls you already satisfy; **(3) the gaps** — assign and work down what's left.

> Don't mark a control **Implemented** until its evidence is attached. "Implemented with no evidence" is the single most common thing that falls apart in an audit.

1.5 Lite vs enterprise: scaling the program

The controls don't change with company size — the cadence, ownership, and rigor do. Use whichever column fits you and move right as you grow.

Dimension	Lite / small company	Enterprise / heavy use
Ownership	One program owner; individuals help on their areas.	A domain owner per Part 2 section; a program lead coordinating.
Cadence	A weekly hour; quarterly access reviews.	Standing weekly review; monthly metrics; quarterly management review.
Forms	The forms in this handbook, kept lightweight.	Living registers in the workspace / GRC tool, with history and audit trail.
Scope	Your core stack and SaaS.	Full asset and vendor inventory; multiple environments; subsidiaries.
Evidence	Screenshots and exports refreshed each cycle.	Automated collection where possible; sampling across the period.
Audit	Type I first, then Type II.	Recurring Type II; multiple frameworks in parallel.

LITE / SMALL COMPANY

If you're small, resist over-engineering. A complete, honest program on the fundamentals beats an elaborate one you can't keep current. Every control still applies — you just keep the paperwork light.

ENTERPRISE / HEAVY USE

At scale, the risk flips to consistency and freshness. Make the forms living registers, automate evidence collection, and review on a fixed cadence so nothing silently goes stale between audits.

PART 2

The control domains

Each domain follows the same shape: its purpose, what good looks like (the instructions), the evidence to collect, and the fillable forms/registers. Attach each item to the matching control in your program (p. 4).

2.1 Governance, policies & risk management

Everything else rests on this: written policies that say what you do, and a risk process that decides where to focus. Auditors read your policies first and check that the rest of the program matches them.

WHAT GOOD LOOKS LIKE

- A complete, approved, and dated policy set — information security, access control, acceptable use, incident response, business continuity, vendor management, and (for HIPAA) privacy and sanctions.
- Policies reviewed at least annually and version-controlled, with an owner for each.
- A documented risk assessment: assets and threats identified, risks rated by likelihood and impact, and a treatment plan for the ones that matter.
- Management sign-off — leadership has reviewed and accepted the program and the residual risk.

EVIDENCE TO COLLECT

- The approved policy documents (with approval date and version).
- The risk assessment and risk treatment / remediation plan.
- Evidence of the annual policy review (a dated record or ticket).
- Management review minutes or sign-off.

> **TIP**
> Attach each item to the matching control in your workspace, and favor dated, system-generated evidence. See Running the program (p. 4) and What compliance evidence is (p. 3).

FORMS & REGISTERS

FORM · POLICY REGISTER

Policy	Owner	Version	Approved	Next review	Location / link

FORM · RISK REGISTER

#	Risk	Likelihood	Impact	Owner	Treatment	Status / review

Rate likelihood and impact Low / Medium / High. Treatment is one of: mitigate, accept (with justification), transfer, or avoid.

2.2 Access control & identity

The most-tested area in every framework. The goal is simple to state and hard to prove: the right people have exactly the access they need, and nobody else — and you can show it.

WHAT GOOD LOOKS LIKE

- Multi-factor authentication enforced on email, VPN, admin consoles, and cloud accounts — no exceptions for admins.
- Access granted through a request-and-approval process, least-privilege by default.
- Access removed promptly on offboarding (same-day for privileged access).
- A periodic access review (usually quarterly) where owners confirm each person still needs their access.
- Unique accounts (no shared logins) and a strong authentication policy.

EVIDENCE TO COLLECT

- MFA configuration screenshots / exports for each system.
- The current user access list per system.
- The most recent completed access review, dated and signed by the reviewer.
- Onboarding and offboarding records showing access granted and revoked.

> **TIP**
> Attach each item to the matching control in your workspace, and favor dated, system-generated evidence. See Running the program (p. 4) and What compliance evidence is (p. 3).

FORMS & REGISTERS

FORM · USER ACCESS REGISTER

User	Role	System	Access level	Granted	Approved by

FORM · QUARTERLY ACCESS REVIEW

System	Reviewer	Date	Users reviewed	Changes made	Sign-off

2.3 Encryption & data protection

Prove that sensitive data is protected in transit and at rest, and that you know where it lives. Encryption is a control auditors can verify quickly — so gaps here stand out.

WHAT GOOD LOOKS LIKE

- TLS enforced on every public endpoint; no plaintext services.
- Disk / volume encryption on servers and laptops.
- Encryption at rest for databases, backups, and object storage.
- A data inventory: what sensitive data you hold, where, and how it's classified.
- Key management: keys stored in a secrets manager / KMS, rotated, and access-controlled.

EVIDENCE TO COLLECT

- Configuration exports showing encryption enabled (disk, DB, storage).
- TLS scan or configuration for public endpoints.
- The data inventory / classification document.
- Key management approach and evidence of rotation.

> **TIP**
> Attach each item to the matching control in your workspace, and favor dated, system-generated evidence. See Running the program (p. 4) and What compliance evidence is (p. 3).

FORMS & REGISTERS

FORM · DATA INVENTORY & CLASSIFICATION

Data type	Classification	Where it lives	Encrypted at rest	In transit	Owner

Classify as Public / Internal / Confidential / Restricted. Restricted includes PHI, cardholder data, and secrets.

2.4 Logging, monitoring & detection

You can't respond to what you can't see. Auditors want evidence that security-relevant events are logged, retained, and actually reviewed — not just collected.

WHAT GOOD LOOKS LIKE

- Central logging from key systems, retained for a defined period.
- Alerting on security events (failed logins, privilege changes, new admin, disabled logging).
- A person or service that reviews and triages alerts — and evidence they do.
- Time synchronization and tamper-resistant storage of logs.

EVIDENCE TO COLLECT

- Logging configuration and the retention setting.
- A sample alert and its configuration.
- A triaged alert or ticket showing review happened.

> **TIP**
> Attach each item to the matching control in your workspace, and favor dated, system-generated evidence. See Running the program (p. 4) and What compliance evidence is (p. 3).

FORMS & REGISTERS

FORM · LOG SOURCE INVENTORY

System	Log type	Destination	Retention	Reviewed by

2.5 Vulnerability & patch management

Show that you find weaknesses and fix them on a schedule. This is where real-world security and audit evidence line up most directly.

WHAT GOOD LOOKS LIKE

- Regular vulnerability scanning (authenticated where possible) on a defined cadence.
- A patch policy with target timelines by severity (e.g., critical within days).
- A tracked remediation process — findings are triaged, assigned, and closed.
- Evidence you closed real findings, not just that you scan.

EVIDENCE TO COLLECT

- Scan schedule and a sample scan report.
- The patch / update policy.
- A remediation ticket showing a finding fixed (before / after or close-out).

> **TIP**
> Attach each item to the matching control in your workspace, and favor dated, system-generated evidence. See Running the program (p. 4) and What compliance evidence is (p. 3).

FORMS & REGISTERS

FORM · VULNERABILITY REMEDIATION TRACKER

Finding / CVE	Severity	Asset	Found	Owner	Due	Status

2.6 Change management

Prove that changes to production are reviewed, tested, and traceable — so a change can't quietly become an outage or a security hole.

WHAT GOOD LOOKS LIKE

- Changes go through review/approval (code review, change ticket, or CAB for larger orgs).
- Testing before production and a rollback plan for significant changes.
- A traceable record — who changed what, when, and why.
- Separation of duties where it matters (the author isn't the sole approver for high-risk changes).

EVIDENCE TO COLLECT

- The change management policy / process.
- An example change with its approval and testing record.
- Evidence of code review or a change ticket trail.

> **TIP**
> Attach each item to the matching control in your workspace, and favor dated, system-generated evidence. See Running the program (p. 4) and What compliance evidence is (p. 3).

FORMS & REGISTERS

FORM · CHANGE LOG

Change	Requested by	Approved by	Tested	Date	Rollback

2.7 Backups, DR & business continuity

Show you can recover. The one piece auditors always ask for — and the one most often missing — is proof of a tested restore, not just that backups exist.

WHAT GOOD LOOKS LIKE

- Backups configured for critical systems and data, on a defined schedule.
- Backups are encrypted and, ideally, immutable / offline copies.
- A tested restore, done at least annually, with a recorded result.
- A business continuity / disaster recovery plan with RTO and RPO targets.

EVIDENCE TO COLLECT

- Backup configuration and schedule.
- A dated restore-test record with the result.
- The BC/DR plan.

> **TIP**
> Attach each item to the matching control in your workspace, and favor dated, system-generated evidence. See Running the program (p. 4) and What compliance evidence is (p. 3).

FORMS & REGISTERS

FORM · BC/DR TEST LOG

System / scenario	Test date	RTO target	Actual	Result	Owner

2.8 Incident response

Prove you're ready to detect, contain, and learn from an incident — before one happens. A plan nobody has rehearsed is a gap.

WHAT GOOD LOOKS LIKE

- A written IR plan with roles, severity levels, and steps.
- Contact paths and escalation defined in advance (including counsel and notification for breaches).
- At least one test or tabletop exercise per year.
- Post-incident reviews that feed back into the program.

EVIDENCE TO COLLECT

- The incident response plan.
- A tabletop or test record.
- A closed incident / ticket showing the process ran end to end.

> **TIP**
> Attach each item to the matching control in your workspace, and favor dated, system-generated evidence. See Running the program (p. 4) and What compliance evidence is (p. 3).

FORMS & REGISTERS

FORM · INCIDENT LOG

#	Date	Summary	Severity	Owner	Actions taken	Closed

2.9 Vendor & third-party risk

Your breach is frequently your vendor's breach. Show you know who holds your and your customers' data, and that you assess them.

WHAT GOOD LOOKS LIKE

- A current inventory of vendors that hold or process your data.
- Security review of key vendors — their SOC 2 / ISO report or a completed questionnaire.
- Contracts with data-processing and breach-notification terms.
- Reassessment on a schedule (annually for critical vendors).

EVIDENCE TO COLLECT

- The vendor inventory.
- Collected vendor reports / questionnaires.
- Contract clauses covering security and breach notification.

> **TIP**
> Attach each item to the matching control in your workspace, and favor dated, system-generated evidence. See Running the program (p. 4) and What compliance evidence is (p. 3).

FORMS & REGISTERS

FORM · VENDOR INVENTORY & REVIEW

Vendor	Data held	Criticality	Report on file	Last reviewed	Next review

2.10 HR & security awareness

People are the largest attack surface. Show that hiring, onboarding, training, and offboarding all handle security consistently.

WHAT GOOD LOOKS LIKE

- Background checks per policy for new hires.
- Security awareness training at hire and at least annually, with completion tracked.
- Signed acceptable-use / confidentiality agreements.
- Onboarding and offboarding checklists that cover access, assets, and training.

EVIDENCE TO COLLECT

- Background-check policy and evidence for recent hires.
- Training completion records.
- Signed agreements; completed onboarding/offboarding checklists.

> **TIP**
> Attach each item to the matching control in your workspace, and favor dated, system-generated evidence. See Running the program (p. 4) and What compliance evidence is (p. 3).

FORMS & REGISTERS

FORM · SECURITY AWARENESS TRAINING LOG

Person	Course	Assigned	Completed	Score / pass

FORM · ONBOARDING / OFFBOARDING CHECKLIST

Person	Type	Access	Assets	Training	Completed

Type = onboarding or offboarding. Offboarding must include same-day removal of privileged access.

2.11 Physical & environmental security

Even cloud-first companies have offices, laptops, and — through their providers — data centers. Show physical access is controlled and the supply chain is covered.

WHAT GOOD LOOKS LIKE

- Controlled physical access to offices and any equipment (badges, logs, visitor sign-in).
- For cloud infrastructure, reliance on providers' physical controls, evidenced by their audit reports.
- Clean-desk / device handling practices; secure disposal of media.

EVIDENCE TO COLLECT

- Office access records / policy.

- Cloud providers' SOC 2 / ISO reports covering physical security.
- Media disposal / device handling policy.

> **TIP**
> Attach each item to the matching control in your workspace, and favor dated, system-generated evidence. See Running the program (p. 4) and What compliance evidence is (p. 3).

FORMS & REGISTERS

FORM · FACILITY & DATA-CENTER RELIANCE

Location / provider	Type	Controls	Evidence

2.12 Asset management

You can't protect what you haven't inventoried. A current asset list underpins access, patching, encryption, and offboarding.

WHAT GOOD LOOKS LIKE

- An inventory of endpoints, servers, and key SaaS applications with owners.
- Each asset tracked through its lifecycle (issue → return → dispose).
- The inventory reconciled periodically against reality.

EVIDENCE TO COLLECT

- The asset inventory (export from your MDM/RMM if you have one).
- Evidence of a reconciliation.

> **TIP**
> Attach each item to the matching control in your workspace, and favor dated, system-generated evidence. See Running the program (p. 4) and What compliance evidence is (p. 3).

FORMS & REGISTERS

FORM · ASSET INVENTORY

Asset	Type	Owner / user	Encrypted	Issued	Status

2.13 HIPAA-specific: PHI, BAAs & breach notification

If you touch protected health information (PHI), HIPAA adds specific duties on top of the security fundamentals above. This section covers what's unique to it.

WHAT GOOD LOOKS LIKE

- A PHI inventory: what PHI you handle, where it flows, and who touches it.
- A signed Business Associate Agreement (BAA) with every vendor that handles PHI on your behalf — and with your covered-entity customers.
- A HIPAA risk analysis (the Security Rule's foundational requirement) and a sanctions policy.
- A breach-notification process aligned to the HIPAA timelines (individuals without unreasonable delay and no later than 60 days; HHS per the rules).

EVIDENCE TO COLLECT

- The PHI inventory / data-flow map.
- The BAA register and copies of signed BAAs.
- The HIPAA risk analysis and sanctions policy.
- The breach-notification procedure.

> **TIP**
> Attach each item to the matching control in your workspace, and favor dated, system-generated evidence. See Running the program (p. 4) and What compliance evidence is (p. 3).

FORMS & REGISTERS

FORM · BAA REGISTER

Party	Role	PHI involved	Signed	Renewal

Role = business associate or covered entity. Track both your upstream customers and your downstream vendors.

PART 3

Framework reference

A quick map of each framework's structure, so you know how the domains in Part 2 line up with what an auditor certifies.

3.1 SOC 2 — Trust Services Criteria

SOC 2 is organized around five Trust Services Criteria categories. **Security** (the "common criteria," CC1–CC9) is always in scope; the other four are optional based on what you commit to.

- **Security** — protection against unauthorized access (the common criteria; maps to most of Part 2).
- **Availability** — the system is available for operation and use as committed (backups, DR, monitoring).
- **Confidentiality** — confidential information is protected (encryption, access, classification).
- **Processing integrity** — processing is complete, valid, accurate, timely, authorized.
- **Privacy** — personal information is handled per your privacy notice.

> **TIP**
> The common criteria are mostly access, change, risk, monitoring, and vendor management — exactly the domains (p. 6) in Part 2. Work those and you've covered the core of SOC 2 Security.

3.2 ISO 27001 — ISMS & Annex A

ISO 27001 certifies two things: that you run an **Information Security Management System** (clauses 4–10 — context, leadership, planning/risk, support, operation, evaluation, improvement) and that you've applied the applicable **Annex A** controls, documented in a **Statement of Applicability (SoA)**.

The 2022 Annex A groups controls into four themes: **Organizational**, **People**, **Physical**, and **Technological** — which map cleanly onto Part 2's governance, HR, physical, and technical domains.

FORM · STATEMENT OF APPLICABILITY (EXCERPT)

Annex A control	Applicable?	Justification	Status

List each Annex A control, whether it applies, and why. The SoA is a required ISO 27001 output.

3.3 HIPAA — Security & Privacy Rule

The HIPAA Security Rule defines safeguards in three groups; there's no certificate, but you must be able to demonstrate each. The Privacy Rule adds duties around use and disclosure of PHI.

- **Administrative safeguards** — risk analysis and management, workforce security, training, sanctions, contingency plan, and BAAs.
- **Physical safeguards** — facility access, workstation and device security, media disposal.
- **Technical safeguards** — access control, audit controls, integrity, authentication, transmission security (encryption).

> **TIP**
> Start HIPAA with the risk analysis — it's the foundational Security Rule requirement — then work the HIPAA-specific domain (p. 13) for PHI inventory, BAAs, and breach notification on top of the shared fundamentals.

PART 4

Master trackers

Two workbook-level trackers that tie the whole program together. In the free workspace these are automatic; on paper, keep them here.

4.1 Master evidence index

One row per control: its status, owner, the evidence attached, and when it was last refreshed. This is what your readiness score is computed from and what your auditor pack exports.

FORM · MASTER EVIDENCE INDEX

Domain	Control	Status	Owner	Evidence	Last updated

Status: not started / in progress / implemented / N/A (with justification). Refresh dated evidence before it expires.

4.2 Program plan & audit timeline

Work backward from your target audit date. Set a milestone per phase and per domain so the gap count has a schedule behind it.

FORM · PROGRAM PLAN

Milestone	Owner	Target date	Status

> A typical path: policies and risk assessment first, then close the technical fundamentals (access, MFA, encryption, logging, backups), then vendor and HR evidence, then a readiness review, then the audit. Type I can precede Type II by a few months.

PART 5

Getting help

5.1 Do it yourself, or have us run it

There are two ways to get compliant, and this handbook supports both.

Do it yourself — free. Create an account at **portal.intsignal.com/compliance**, pick a framework, and work the program using this handbook as your guide. The workspace turns every form here into a fillable control with an encrypted evidence vault, live readiness scoring, tasks and reminders, and a one-click auditor export. It's free, with no purchase required, and your evidence is isolated and encrypted — even intSignal admins can't see it.

Have intSignal run it for you. If you'd rather not run it yourself, our team can operate the whole program as a managed / virtual-CISO engagement — mapping controls to your environment, gathering evidence, closing gaps, and preparing you for the audit. You keep the same workspace and see everything as it happens. Talk to our team at **intsignal.com/contact**.

> Full online docs, this handbook, and the workspace all live at **intsignal.com/compliance**. This document is guidance, not legal advice; confirm your specific obligations with your auditor or counsel.