HALE CONSULTING SOLUTIONS LLC

Preparing for SOC 2: What Healthcare AI and Digital Health Vendors Need to Know

Prepared for healthcare technology, digital health, SaaS, and AI-enabled clinical solution providers considering SOC 2 readiness, audit preparation, and attestation strategy

Executive Summary

Healthcare technology vendors, AI-enabled clinical platforms, digital health companies, and EHR-integrated solution providers are facing increasing scrutiny from hospitals, health systems, payers, investors, and enterprise procurement teams. These stakeholders increasingly expect vendors to demonstrate a mature, independently assessed security and operational control environment.

For healthcare technology vendors, a SOC 2 report can become a powerful market-enablement tool. It helps answer a key buyer question:

> "Can we trust this vendor to securely operate systems that process, transmit, store, or support sensitive customer, clinical, or business data?"

SOC 2 is not a HIPAA certification, penetration test, legal opinion, or regulatory approval. Rather, it is an independent attestation report issued by a qualified CPA firm that evaluates the design and, for Type II, operating effectiveness of controls relevant to selected Trust Services Criteria.

SOC 2 Is Especially Valuable For:

- Hospital security review
- Procurement due diligence
- Enterprise contracting
- Investor confidence
- Customer assurance

The Most Practical Path:

Readiness Assessment → Remediation → SOC 2 Type I → SOC 2 Type II

Organizations that treat SOC 2 as an **operational maturity program**, rather than a checkbox audit, gain the most value from the process.

What Is SOC 2?

SOC stands for System and Organization Controls. SOC reports are part of the AICPA's assurance reporting framework for service organizations. A SOC 2 report evaluates controls at a service organization using the AICPA's Trust Services Criteria.

Trust Services Category	What It Addresses
Security	Protection of systems and information against unauthorized access, unauthorized disclosure, and damage
Availability	Whether systems are available for operation and use as committed or agreed
Processing Integrity	Whether system processing is complete, valid, accurate, timely, and authorized
Confidentiality	Whether confidential information is protected as committed or agreed
Privacy	Whether personal information is collected, used, retained, disclosed, and disposed of according to commitments and applicable privacy principles

For most healthcare SaaS, digital health, and healthcare AI vendors, the most common starting scope is **Security**, often with **Availability** and **Confidentiality** added depending on customer expectations. Privacy and Processing Integrity may also be appropriate, but they increase the complexity and evidence burden.

Why SOC 2 Matters for Healthcare AI and Digital Health Vendors

Healthcare organizations are risk-sensitive buyers. Hospitals, academic medical centers, payers, and enterprise health systems often require vendors to provide evidence of security maturity before allowing access to production systems, EHR integrations, PHI, sensitive clinical data, or internal networks.

Hospital Procurement

Reduces friction during security review and vendor onboarding processes

Enterprise Contracting

Demonstrates control maturity to legal, compliance, and IT teams

EHR Integration

Supports trust around identity, access, audit logging, and data handling

AI Governance

Provides an assurance foundation, even though SOC 2 is not AI-specific

Investor Diligence

Shows operational maturity and enterprise readiness

Competitive Positioning

Differentiates the company from less mature vendors

For vendors selling into healthcare, SOC 2 is not just a compliance artifact. It is part of the **trust package** needed to move through enterprise due diligence.

SOC 2 Is Not the Same as HIPAA Compliance

SOC 2 and HIPAA overlap, but they are not interchangeable. Understanding the distinction is critical for healthcare technology vendors navigating both frameworks.

Topic	HIPAA	SOC 2
Primary purpose	Protect PHI/ePHI and support regulatory compliance	Provide independent assurance over controls relevant to selected Trust Services Criteria
Governing source	Federal law and regulation	AICPA attestation framework
Applies to	Covered entities, business associates, subcontractor business associates	Service organizations seeking independent assurance
Output	Risk analysis, policies, procedures, compliance evidence	CPA-issued SOC 2 report
Certification?	No official HIPAA certification by OCR	SOC 2 report issued by independent CPA firm
Focus	Regulatory safeguard compliance	Control design and operating effectiveness

HIPAA readiness asks: "Do you have reasonable safeguards for protecting PHI?"

SOC 2 Type II asks: "Can you prove your selected controls operated effectively over a defined period?"

A HIPAA risk assessment is a strong foundation for SOC 2 readiness. However, SOC 2 Type II requires documented evidence that controls operated **consistently over time** — something HIPAA readiness assessments often do not require.

SOC 2 Type I vs. SOC 2 Type II

SOC 2 reports come in two primary forms. Understanding the difference is essential for planning your assurance journey.

SOC 2 Type I

Evaluates whether controls are **suitably designed at a specific point in time**.

It answers: "Are the right controls designed and in place as of the audit date?"

Type I is useful when an organization is early in its assurance journey and wants to demonstrate that it has established a control environment. It does not prove that controls operated effectively over a period of time.

SOC 2 Type II

Evaluates both whether controls are suitably designed **and** whether those controls operated effectively over a defined review period.

It answers: "Did the controls operate consistently and effectively over time?"

Schellman describes Type II SOC examinations as reports on operational controls, including both the suitability of design and operating effectiveness of controls over a specified period.

Feature	SOC 2 Type I	SOC 2 Type II
Evaluation period	Point in time	Period of time
Focus	Control design	Control design and operating effectiveness
Evidence burden	Moderate	High
Time to complete	Shorter	Longer
Best for	First-time SOC 2 readiness, early customer assurance	Mature customer assurance, enterprise procurement
Customer value	Good starting point	Stronger assurance

For many healthcare technology vendors, the recommended path is: **SOC 2 Type I first, then SOC 2 Type II after 3–6 months of operating evidence.** This gives the company a near-term assurance milestone while building the evidence base needed for Type II.

Who Performs the SOC 2 Audit?

A SOC 2 report must be issued by an independent CPA firm qualified to perform SOC attestation engagements. Advisory firms, compliance consultants, virtual CISOs, and readiness consultants can help prepare the organization, but they should not represent themselves as the independent SOC 2 auditor unless they are a qualified CPA firm performing the attestation.

Company Management

Owns the system, controls, commitments, and representations

Readiness Advisor

Helps scope, prepare, map controls, organize evidence, and remediate gaps

Control Owners

Operate and document controls throughout the review period

CPA Audit Firm

Performs the independent SOC 2 examination and issues the report

Customers / Prospects

Review the SOC 2 report under NDA or controlled distribution

⚠ A readiness advisor can help prepare the organization, but the **independent SOC 2 report must come from the CPA audit firm**. These roles must remain clearly separated.

What Is Involved in Preparing for SOC 2?

SOC 2 preparation is more than filling out a questionnaire. It is a structured readiness, control design, evidence, and audit process. A typical SOC 2 readiness program includes the following workstreams.

01

Define the System Scope

Identify what system or service is covered: production SaaS platform, cloud infrastructure, EHR integration components, AI processing workflows, identity and access management, and vendor/subprocessor dependencies. Scope clarity is critical — overly narrow scope may disappoint customers; overly broad scope creates unnecessary audit complexity.

02

Select the Trust Services Criteria

Security is generally included in every SOC 2 report. Availability is strongly recommended if customers depend on system uptime. Confidentiality is strongly recommended if sensitive data is handled. Privacy and Processing Integrity should be considered carefully based on risk profile. For many first-time healthcare SaaS vendors, **Security + Availability + Confidentiality** is a practical first scope.

03

Document the Control Environment

Document policies, procedures, technical controls, governance processes, and operational practices that support the SOC 2 scope — including governance, access control, change management, system operations, risk management, vendor management, incident response, and AI-specific controls.

04

Build a SOC 2 Control Matrix

Map Trust Services Criteria to risks, control activities, control owners, frequency, evidence required, systems/tools used, related policies, testing expectations, and gaps. This becomes the operating blueprint for readiness and audit preparation.

05

Collect Evidence

Evidence is the heart of SOC 2, especially Type II. For Type I, evidence demonstrates controls are designed and in place. For Type II, evidence must demonstrate controls operated over the review period — including policies, access records, change logs, monitoring evidence, vendor documentation, training records, and incident response evidence.

Documenting the Control Environment

The organization must document the policies, procedures, technical controls, governance processes, and operational practices that support the SOC 2 scope. This commonly includes the following areas:

Governance

- Security roles and management oversight
- Risk management and policy review

Access Control

- MFA, RBAC, least privilege
- Onboarding, offboarding, access reviews

Change Management

- Code review and change approval
- Deployment controls and rollback procedures

System Operations

- Monitoring, logging, alerting
- Incident response and backup operations

Vendor Management

- Subprocessor review and contracts
- Security documentation and DPAs

AI-Specific Controls

- Model governance and prompt handling
- Human oversight and output monitoring

SOC 2 Area	Control Example	Evidence Example
Access control	Privileged access is reviewed quarterly	Access review report, signoff, remediation tickets
Change management	Production changes require review and approval	Pull requests, deployment logs, approval records
Incident response	Security incidents are tracked and escalated	Incident tickets, after-action reports
Vendor management	Critical vendors are reviewed annually	Vendor risk assessments, SOC reports, DPAs
Availability	Backups are performed and tested	Backup logs, restore test results
Confidentiality	Sensitive data is encrypted in transit and at rest	Architecture diagrams, encryption settings, cloud configuration evidence

Evidence Collection: The Heart of SOC 2

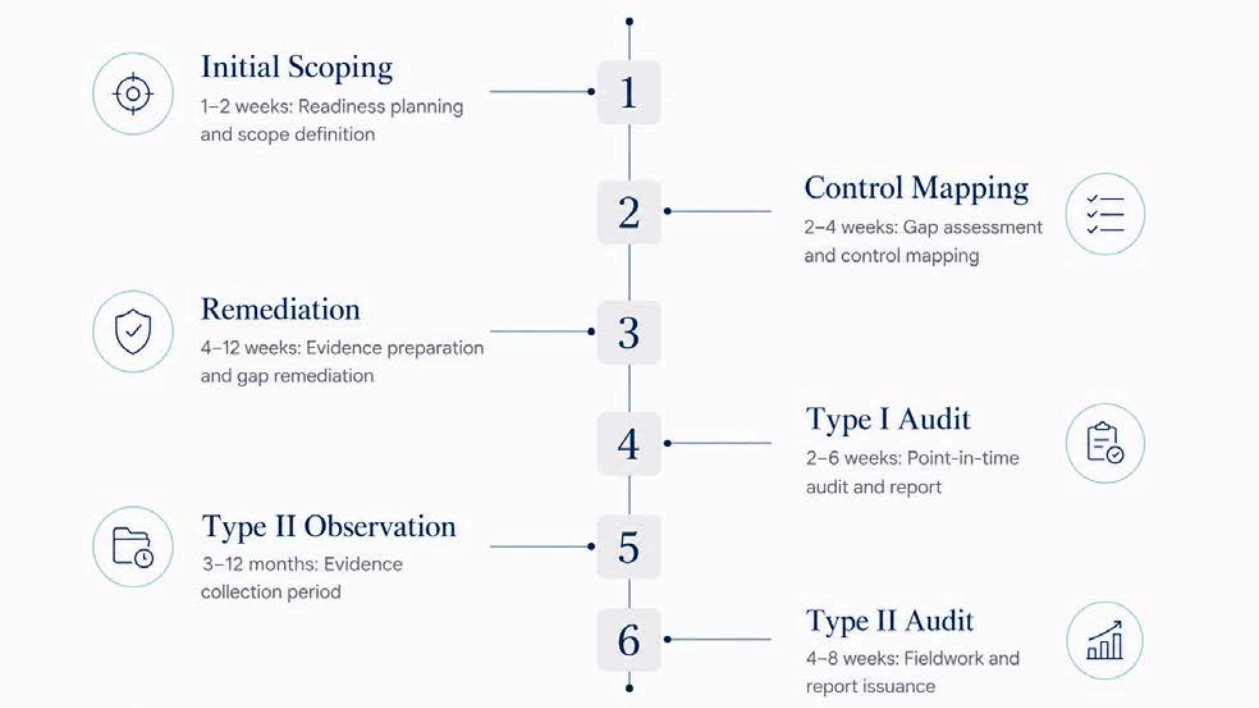
Evidence is the heart of SOC 2, especially Type II. For Type I, evidence demonstrates that controls are designed and in place at a point in time. For Type II, evidence must demonstrate that controls operated over the review period. For companies that have never operated in an audit evidence discipline before, this is often the most challenging part.

Evidence Category	Examples
Policies	Information security policy, access control policy, incident response plan
Governance records	Risk assessments, management review, control owner signoff
Access evidence	MFA settings, access reviews, user provisioning/deprovisioning records
Change evidence	Pull requests, code review records, deployment logs, change tickets
Monitoring evidence	SIEM alerts, uptime reports, logging configuration, incident tickets
Vendor evidence	Vendor risk assessments, contracts, SOC reports, BAA/DPA records
Training evidence	Security training completion, HIPAA training, policy acknowledgments
Backup/recovery evidence	Backup logs, restoration tests, RTO/RPO documentation
Vulnerability evidence	Scan results, remediation tickets, penetration test summary
Incident response evidence	Incident register, tabletop report, lessons learned, escalation matrix

⚠ Common readiness gaps include: informal access reviews, undocumented change management, incomplete vendor management, no formal risk register, weak incident response evidence, no restore testing, and missing control owners. These must be addressed before audit.

Typical Timeline and Roadmap

The timeline depends on maturity, scope, resource availability, and whether the organization starts with Type I or goes directly to Type II.



Month	Activity
Month 1	SOC 2 scoping, readiness assessment, control mapping
Month 2	Remediation planning, evidence repository, policy updates
Month 3	Type I audit readiness and possible Type I audit
Months 4–9	Type II evidence collection period
Months 10–11	Type II audit fieldwork
Month 12	Type II report issuance and customer distribution process

A faster path may be possible if the organization already has mature policies, automated evidence collection, formal access reviews, vulnerability management, vendor review, and change management.

Typical Work Effort

SOC 2 readiness is usually a cross-functional effort involving security, engineering, operations, leadership, legal, compliance, HR, vendor management, and customer success.

40–60

Light Review

Advisory hours for mature organizations with strong existing evidence

75–120

Standard Engagement

Advisory hours for typical first-time SOC 2 candidates

120–200+

Full Readiness

Advisory hours for early-stage companies needing policies, SOPs, and evidence discipline

10–30

Ongoing Type II

Monthly advisory hours for companies collecting Type II evidence

Readiness Level	Advisory Effort	Internal Team Effort	Suitable For
Light readiness review	40–60 hours	40–80 hours	Mature organization with strong existing evidence
Standard readiness engagement	75–120 hours	100–200 hours	Typical first-time SOC 2 candidate
Full readiness plus remediation	120–200+ hours	200–400+ hours	Early-stage company needing policies, SOPs, and evidence discipline
Ongoing Type II support	10–30 hours/month	20–60 hours/month	Company collecting Type II evidence over 3–12 months

The largest variable is not the audit itself. The largest variable is **how much remediation and evidence creation must happen before the audit**.

Common Readiness Gaps

First-time SOC 2 candidates often underestimate the level of operational evidence required. The following gaps are frequently identified during readiness assessments and must be addressed before entering the formal audit process.

Informal Access Reviews

SOC 2 requires evidence of periodic review and remediation — not just a stated policy

Undocumented Change Management

Auditors need proof of review, approval, testing, and deployment control for every production change

Incomplete Vendor Management

Critical vendors and subprocessors must be evaluated and monitored with documented evidence

No Formal Risk Register

Risk assessment should be documented and maintained — not just performed informally

Weak Incident Response Evidence

A written plan is not enough; organizations need incident logs and tabletop exercises

No Restore Testing

Backup existence is weaker than proven recovery capability — restore tests must be documented

Incomplete Onboarding/Offboarding Evidence

User lifecycle controls must be traceable with documented provisioning and deprovisioning records

Policies Not Acknowledged

Policies should be communicated and acknowledged by employees and contractors

Missing Control Owners

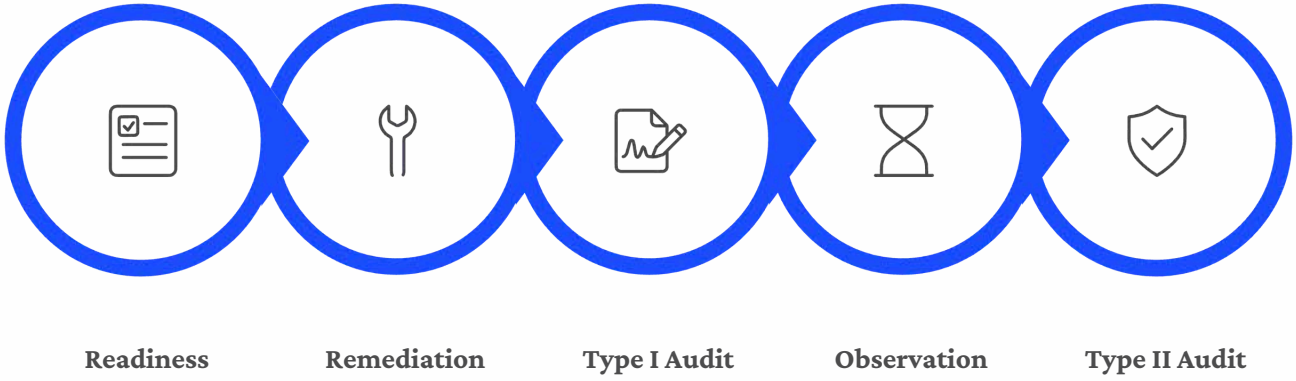
Controls must have accountable owners who are responsible for operation and evidence

No Evidence Calendar

Type II evidence must be collected consistently over time — ad hoc collection is insufficient

Recommended SOC 2 Path for Healthcare AI and Digital Health Vendors

The most practical path is usually phased. Each phase builds on the previous, creating a structured journey from initial assessment to a fully issued Type II report.



This phased approach allows leadership to make informed decisions at each stage about budget, timeline, scope, and readiness before committing to the next phase.

Phase 1: Readiness Assessment

Objective: Determine current readiness and define the path forward.

- Confirm system scope and select Trust Services Criteria
- Map existing controls and review policies
- Identify evidence gaps and build remediation roadmap
- Recommend Type I vs. Type II sequencing

Deliverables: SOC 2 readiness report, control matrix, evidence request list, gap/remediation roadmap, recommended audit timeline

Phase 2: Remediation and Evidence Preparation

Objective: Prepare the control environment for audit.

- Assign control owners and update policies/SOPs
- Build evidence repository and implement missing review processes
- Formalize access reviews and validate backup/restore procedures
- Conduct incident tabletop and document vendor reviews
- Establish evidence calendar

Deliverables: Updated policies, evidence repository structure, control owner matrix, audit-ready evidence index, remediation tracker

SOC 2 Type I and Type II Audit Phases

Phase 3: SOC 2 Type I Audit

Objective: Demonstrate that controls are designed and in place.

- Select CPA audit firm
- Submit system description
- Provide control matrix and point-in-time evidence
- Respond to auditor requests
- Address exceptions or clarifications

Deliverable: SOC 2 Type I Report

Phase 4: Type II Observation Period

Objective: Operate controls consistently over the audit period.

- Perform recurring access reviews
- Track changes and approvals
- Monitor vulnerabilities and maintain incident records
- Review vendors and collect training records
- Perform management reviews and maintain risk register
- Document exceptions and remediation

Deliverables: Monthly evidence package, exception log, control operation records, updated readiness tracker

Phase 5: SOC 2 Type II Audit

Objective: Obtain independent validation of control design and operating effectiveness.

Provide Evidence Samples

Supply auditors with representative evidence from across the observation period

Support Walkthroughs

Walk auditors through control processes and system architecture

Respond to Testing

Address auditor testing requests and clarify exceptions promptly

Review Draft Report

Review and prepare customer communication strategy before distribution

Deliverable: SOC 2 Type II Report — the gold standard for enterprise customer assurance

Special Considerations for Healthcare AI Vendors

SOC 2 was not designed specifically for AI governance, clinical safety, HIPAA, or FDA considerations. However, healthcare AI vendors should use SOC 2 as part of a broader assurance strategy.

Area	Consideration
PHI/ePHI handling	SOC 2 should align with HIPAA safeguards and BAA commitments
EHR integration	Access scopes, identity context, audit logs, and least privilege must be clear
AI model governance	Prompt handling, model provider use, no-training commitments, and oversight should be documented
Clinical safety	SOC 2 does not validate clinical efficacy or safety — separate validation is required
Vendor chain	Cloud, AI, hosting, support, and subprocessor roles must be mapped
Customer responsibility	Shared responsibility model should be explicit in customer agreements
Data residency	Especially important when international support or subprocessors are involved
Claims governance	Security and AI capability claims should be substantiated
Incident response	Must include security, privacy, PHI, and AI-output-related scenarios

SOC 2 should be coordinated with **HIPAA readiness, enterprise procurement readiness, AI governance, and customer contracting strategy** as part of a comprehensive assurance program.

How Hale Consulting Solutions Can Support the Process

Hale Consulting Solutions is well positioned to help healthcare AI and digital health vendors prepare for SOC 2 by serving as a readiness and audit-preparation advisor.

Appropriate HCS Support Includes:

- SOC 2 readiness assessment and HIPAA-to-SOC 2 control crosswalk
- Trust Services Criteria scoping and evidence gap analysis
- Control matrix development and policy/SOP review
- Risk register development and vendor/subprocessor evidence review
- Incident tabletop facilitation and backup/recovery evidence review
- Healthcare procurement assurance package development
- Auditor selection support, audit coordination, and Type II evidence calendar support

Practical Readiness Checklist Highlights

Governance: Assigned security owners, current policies, periodic risk assessments, risk register

Access Control: MFA enforced, roles documented, access reviews performed, privileged accounts monitored

Change Management: Code changes reviewed, deployments approved, emergency changes documented

System Operations: Logs monitored, incidents tracked, vulnerabilities scanned, backups tested

Vendor Management: Critical vendors identified, contracts/BAAs/DPAs maintained, subprocessors tracked

Audit Readiness: Evidence repository established, control owners assigned, evidence calendar in place

Important Independence Note: HCS supports SOC 2 readiness, control mapping, evidence preparation, and audit coordination. The independent SOC 2 report must be issued by a qualified CPA audit firm.

Selecting a SOC 2 Audit Firm

Once the organization has completed its readiness assessment and understands its likely SOC 2 scope, the next step is selecting an independent CPA audit firm to perform the SOC 2 examination. Organizations should consider obtaining quotes from firms at different price points to compare cost, credibility, audit style, timeline, and fit.

VALUE / STARTUP-FRIENDLY

Johanson Group LLP

A licensed CPA firm providing SOC 2 readiness assessments, examinations, and audits.
Best fit: Organizations pursuing their first SOC 2 Type I or Type II that want a practical audit experience without paying premium enterprise-audit pricing.
Potential limitation: May not carry the same enterprise-recognition weight as larger firms when selling into highly sophisticated enterprise buyers.

MID-MARKET / HEALTHCARE-CAPABLE

BARR Advisory

Provides SOC 1, SOC 2, SOC 3, and SOC for Cybersecurity services.
Best fit: Healthcare SaaS, cloud, and growth-stage technology vendors looking for a balance of credibility, responsiveness, and cost.
Potential limitation: Likely more expensive than smaller startup-friendly CPA firms.

MID-MARKET / MULTI-FRAMEWORK

A-LIGN

A widely recognized cybersecurity compliance and assurance provider offering SOC 2, ISO 27001, HITRUST, FedRAMP, and PCI services.
Best fit: Growth-stage healthcare technology vendors that want a recognized audit partner and may later pursue HITRUST, ISO 27001, FedRAMP, or other assurance programs.
Potential limitation: May be more process-heavy and expensive than a smaller CPA firm.

PREMIUM / ENTERPRISE-GRADE

Schellman

One of the most recognized names in SOC and security attestation, issuing more than 2,000 SOC reports each year.
Best fit: Organizations selling into large health systems, payers, enterprise customers, or highly security-sensitive environments where auditor brand recognition may influence customer confidence.
Potential limitation: Likely to be more expensive and more rigorous.

Selecting a SOC 2 Audit Firm

Key Questions to Ask Each Audit Firm:

- Proposed SOC 2 Type I and Type II pricing
- Recommended Trust Services Criteria scope
- Estimated audit timeline and expected evidence requirements
- Experience with healthcare SaaS or digital health clients
- Whether readiness and audit services are separated appropriately
- How they handle auditor independence
- Expected customer support during audit fieldwork
- Report delivery timeline after fieldwork
- Additional fees for scope changes or retesting

The key is not simply choosing the cheapest or most recognizable firm. The right audit partner should match the organization's **maturity, customer expectations, budget, timeline, and long-term assurance roadmap**.

Conclusion

SOC 2 can be a valuable enterprise assurance milestone for healthcare AI and digital health vendors. It helps demonstrate that the organization has designed and operated controls to protect customer systems and information in accordance with recognized trust criteria.

For healthcare technology vendors, SOC 2 is not merely a compliance exercise. It is a **market-readiness asset**. It can reduce hospital procurement friction, strengthen customer confidence, improve security discipline, and support enterprise growth.

1

Readiness Assessment

Scope, gap analysis, control mapping

2

Remediation

Policies, evidence, control owners

3

SOC 2 Type I

Point-in-time control design validation

4

SOC 2 Type II

Operating effectiveness over time

Organizations that treat SOC 2 as an **operational maturity program**, rather than a checkbox audit, will gain the most value from the process. The recommended next step is a SOC 2 Readiness and Audit Preparation Engagement before committing to a formal Type II audit.

The initial engagement should produce: SOC 2 scope recommendation, Type I vs. Type II roadmap, Trust Services Criteria recommendation, control matrix, evidence request list, gap assessment, remediation roadmap, audit timeline, estimated internal resource plan, and auditor selection support strategy. This allows leadership to make an informed decision about budget, timeline, scope, and readiness before entering the formal audit process.