Axiom Sovereign

TECHNOLOGY SOVEREIGNTY ADVISORY

COMPLIANCE FRAMEWORK SERVICE — PLANNING GUIDE

Compliance Program Timeline Planner

NIST CSF · SOC 2 · HIPAA · NIST 800-171 · Realistic Timelines

v1.0 — 2026

Axiom Sovereign LLC · Severna Park, MD · info@axiomsovereign.com · axiomsovereign.com

Compliance Program Timeline Planner

How Long Does Compliance Actually Take?

The most common question from organizations beginning a compliance journey is: "How long will this take?" The honest answer depends on your starting point, organizational resources, and the specific framework. This planner provides realistic timeline estimates for the five frameworks most commonly required by mid-market professional services organizations, along with the factors that accelerate or delay each.

The Two Variables That Matter Most

1. Your current maturity level: An organization with documented policies, MFA deployed, and an active risk management process can achieve SOC 2 in 4–6 months. An organization starting from scratch needs 9–14 months. Know your baseline before committing to a timeline.

2. Dedicated execution vs. advisory-only: Organizations that have someone executing — implementing controls, writing policies, managing evidence — consistently hit timelines. Organizations that receive recommendations and must implement themselves on top of existing workloads consistently take 2–3x longer. This is the core argument for a hands-on vCISO engagement over a compliance advisory-only relationship.

NIST CSF 2.0 — PROGRAM DEVELOPMENT

Developing a cybersecurity program aligned to NIST CSF 2.0 is the most common starting point for mid-market organizations. It is not a certification — it is a framework for organizing and maturing your security program.

Realistic Timeline: 3–6 months to functional program | 12–18 months to mature program

Phase	Duration	Key Activities
Phase 1: Assessment and Baseline	1–3 weeks	Complete NIST CSF maturity assessment. Score all 22 categories. Identify current vs. target maturity gaps. Produce prioritized roadmap.
Phase 2: Foundation Building	4–8 weeks	Deploy foundational controls: MFA, asset inventory, basic security policy, patch management process, backup verification.
Phase 3: Program Documentation	6–12 weeks	Develop core policy library: Information Security Policy, Incident Response Plan, Acceptable Use Policy, Vendor Management Policy. Risk register populated.

Phase	Duration	Key Activities
Phase 4: Governance and Monitoring	8–16 weeks	Establish ongoing governance: advisory cadence, risk register review, security awareness training, quarterly access reviews, log monitoring.
Phase 5: Ongoing Maturity	Ongoing	Quarterly review, annual reassessment, program improvement based on incidents and regulatory changes.

• Existing IT team to implement controls • Prior security investment (some policies exist) • Leadership commitment to dedicated time • vCISO executing rather than just advising	• No internal IT resources for implementation • Starting from zero with no existing policies • Competing priorities limiting staff time • Advisory-only engagement requiring self-implementation

SOC 2 TYPE II — CERTIFICATION

SOC 2 Type II is an audited certification covering a minimum 6-month observation period. The timeline begins with pre-audit readiness work and ends with the auditor's report. Plan for 9–18 months from start to report.

Realistic Timeline: Well-prepared organization: 9–12 months from start | Starting from scratch: 14–18 months

Phase	Duration	Key Activities
Phase 1: Gap Assessment	2–4 weeks	Complete SOC 2 readiness self-assessment (this document). Identify all control gaps against the Trust Services Criteria selected.
Phase 2: Remediation	8–16 weeks	Implement all controls required to meet selected Trust Services Criteria. Document evidence. Most organizations underestimate this phase.
Phase 3: Readiness Review	2–4 weeks	Internal or vCISO-led review of all controls before engaging auditor. Identify remaining gaps. Fix anything not audit-ready.
Phase 4: Auditor Selection and Engagement	2–4 weeks	Issue RFP to 2–3 AICPA-accredited CPA firms. Select auditor. Execute engagement agreement. Establish observation start date.
Phase 5: Type I Assessment (Optional)	4–6 weeks	Point-in-time assessment of control design. Not required but recommended for organizations with significant gaps or first-time certifications.
Phase 6: Type II Observation Period	6–12 months	Auditor observes controls operating consistently over the observation period. Evidence collected monthly. Any control failures must be documented and addressed.
Phase 7: Audit Fieldwork and Report	6–10 weeks	Auditor conducts fieldwork, tests evidence, conducts interviews. Management responses to findings. Draft report review. Final report issued.

• High pre-readiness maturity (75%+ controls implemented) • Dedicated compliance owner managing evidence collection • GRC platform for evidence management • Axiom Sovereign executing controls and managing evidence	• Gaps discovered during observation period requiring mid-audit remediation • Key staff unavailable for auditor interviews • Evidence not maintained consistently during observation period • Scope creep (adding Trust Services Criteria mid-engagement)

HIPAA SECURITY RULE — FULL COMPLIANCE

HIPAA compliance is not a certification — it is an ongoing obligation for covered entities and business associates. The timeline covers developing a compliant program from an assessed baseline.

Realistic Timeline: Basic compliance foundation: 3–4 months | Full compliant program: 6–9 months

Phase	Duration	Key Activities
Phase 1: Risk Analysis	2–4 weeks	Conduct HIPAA Security Risk Analysis per 45 CFR §164.308(a)(1). Document all ePHI systems, threats, vulnerabilities, likelihood, and impact.
Phase 2: Risk Management Plan	1–2 weeks	Document risk management decisions for each identified risk. Assign owners and remediation timelines.
Phase 3: Policy Development	4–8 weeks	Develop all required HIPAA policies: Security Management, Access Control, Audit Controls, Breach Notification, Sanction Policy, Workforce Training.
Phase 4: Technical Safeguards	4–12 weeks	Implement: MFA, access controls, audit logging, encryption of PHI at rest and in transit, BAAs with all applicable vendors.
Phase 5: Training and Awareness	2–4 weeks	Deploy HIPAA training to all workforce members. Document completion. Establish annual recertification.
Phase 6: Ongoing Compliance	Ongoing	Annual risk analysis, BAA reviews, policy updates, workforce training, breach response readiness.

• EHR system already has HIPAA-compliant configuration • Prior training programs in place • Small workforce (faster training deployment) • vCISO completing risk analysis and writing policies	• Large number of systems containing ePHI • Multiple locations requiring separate risk analysis components • Legacy systems without encryption support • Vendors unwilling to execute BAAs (requires vendor replacement)

NIST SP 800-171 — CUI PROTECTION (CMMC PREP)

NIST SP 800-171 covers the protection of Controlled Unclassified Information (CUI) in non-federal systems. Compliance is required by federal contracts and is the foundation for CMMC Level 2 certification.

Realistic Timeline: Self-assessment and POAM: 2–3 months | Full CMMC Level 2 certification: 12–24 months

Phase	Duration	Key Activities
Phase 1: CUI Identification	1–3 weeks	Identify all systems, locations, and processes that handle CUI. Establish CUI boundary. Determine if a System Security Plan (SSP) is required.
Phase 2: Self-Assessment (SPRS Score)	2–4 weeks	Complete NIST SP 800-171 self-assessment against all 110 security requirements. Calculate and submit SPRS score.
Phase 3: Plan of Action and Milestones (POAM)	1–2 weeks	Document all requirements not yet met in a formal POAM with owners and remediation timelines.

Phase	Duration	Key Activities
Phase 4: System Security Plan (SSP)	3–6 weeks	Develop SSP documenting how each of the 110 requirements is met. Required for CMMC Level 2.
Phase 5: Control Implementation	8–20 weeks	Implement all open POAM items. Configuration management, access control, incident response, media protection, personnel security.
Phase 6: C3PAO Assessment (CMMC Level 2)	3–6 months from assessment request	Third-party assessment organization (C3PAO) conducts formal CMMC Level 2 assessment. Remediation of any findings.

• Small CUI environment (limited systems) • Prior security investment addressing many 800-171 requirements • Existing SSP or documentation from prior assessment • Experienced vCISO familiar with 800-171 and CMMC

• Large or complex IT environment with many CUI touchpoints • No prior 800-171 assessment — starting SPRS score from zero • C3PAO availability (assessment backlogs can be 3–6 months) • Subcontractors requiring their own compliance

Ready to Get Started?

Axiom Sovereign executes compliance programs — not just advises on them. We complete your risk analysis, write your policies, implement your controls, and manage your evidence. Engagements mobilize within 5 business days. calendly.com/cmissimore-6zkc/30min · info@axiomsovereign.com