

vCISO Engagement: 30-Day Onboarding

Week-by-Week Activities · Deliverables · Sign-Off Checklist

v1.0 — 2026

vCISO Engagement: 30-Day Onboarding Checklist

About This Document

One of the most common questions from prospective vCISO clients is: "What happens in the first 30 days?" This checklist answers that question completely. It describes every activity, deliverable, and decision point in the Axiom Sovereign onboarding process — organized by week — so you know exactly what to expect and what you will have in hand at the end of the first month.

The onboarding process is designed to deliver immediate, tangible value from day one. By the end of week one, you will have a complete picture of your current security posture. By the end of week four, you will have a documented risk register, a prioritized 90-day roadmap, and a program foundation that would have taken months to build independently.

What You Have After 30 Days

- ✓ Technology Sovereignty Risk Assessment — scored baseline across AI governance, regulatory, and cybersecurity domains
- ✓ Asset inventory — complete list of systems, cloud services, and data repositories
- ✓ Risk register — populated with identified risks, severity ratings, owners, and timelines
- ✓ 90-day remediation roadmap — prioritized action plan tied to assessment findings
- ✓ Policy gap list — which policies you have, which you are missing, and what to build first
- ✓ Regulatory exposure summary — which regulations apply and where the gaps are
- ✓ Quick win action list — 5–10 items that can be implemented in under 30 days at minimal cost

WEEK 1: DISCOVERY AND ASSESSMENT (DAYS 1–7)

The first week is entirely focused on understanding your environment. No recommendations, no action items — just discovery. The goal is to build a complete, accurate picture before any prescriptions are made.

Day 1–2: Kickoff and Access

- Kickoff call with primary contact and key stakeholders (60 minutes)
- Review of current IT environment, cloud services, and major systems
- Collection of existing security policies, prior assessments, and audit reports
- Access to Microsoft 365 / Google Workspace admin console (read-only review)
- Review of current cyber insurance policy and most recent renewal application
- Introduction to staff who will be key contacts during the engagement

Day 3–5: Technical and Regulatory Review

- Review of current security configurations in email, cloud, and endpoint systems
- Review of existing vendor contracts for security and data protection terms
- Identification of applicable regulations based on industry, data types, and geographies
- Review of prior incident history and any open audit or regulatory findings
- Initial shadow AI discovery — review of approved and unapproved AI tool usage

Day 6–7: Assessment Scoring

- Complete Technology Sovereignty Risk Assessment across all three domains
- Score each control against assessment criteria
- Identify all items scored 0 (not addressed) as priority gap list
- Draft preliminary risk register with initial risk ratings

WEEK 2: FINDINGS AND ROADMAP DEVELOPMENT (DAYS 8–14)

Week two translates the discovery findings into a prioritized action plan. You will receive your assessment results, understand exactly where you stand, and have a clear picture of what needs to happen and in what order.

Day 8–10: Assessment Delivery

- Delivery of completed Technology Sovereignty Risk Assessment document
- Findings briefing call with primary contact (60 minutes) — walk through every section
- Discussion of risk ratings and prioritization logic
- Identification of quick wins — items that can be addressed immediately at low cost
- Regulatory exposure summary — which obligations are not currently met and the risk they create

Day 11–14: 90-Day Roadmap Development

- Development of 90-day prioritized remediation roadmap tied to assessment findings
- Sequencing of actions based on risk level, effort, and dependencies
- Assignment of owners for each action item (Client vs. vCISO vs. IT)

- Budget estimates for any tools or services required
 - Delivery of roadmap document for Client review and feedback
-

WEEK 3: FOUNDATION BUILDING (DAYS 15–21)

Week three begins execution. The focus is on establishing the foundational program infrastructure — the governance structures, documentation systems, and high-priority quick wins — that everything else builds on.

Program Infrastructure

- Risk register finalized and delivered — populated with all identified risks
- Policy gap analysis completed — inventory of existing policies and priority gaps
- Establish program documentation structure (where policies, evidence, and records live)
- Define advisory session cadence and agenda template for ongoing engagements
- Begin drafting first-priority policies identified in gap analysis

Quick Win Execution

- Work with IT to address 0-cost/low-effort quick wins from assessment (e.g., MFA gaps, admin account cleanup)
 - Provide vendor contract language for next vendor contract renewal
 - Review cyber insurance policy for coverage gaps and document findings
 - Identify staff for security awareness training deployment
-

WEEK 4: FORMAL PROGRAM LAUNCH (DAYS 22–30)

Week four completes the onboarding phase and transitions the engagement into steady-state operations. By the end of this week, the program is active, documented, and running.

Deliverable Finalization

- Deliver final 90-day roadmap incorporating Client feedback from Week 2
- Complete initial policy drafts for Client review (Information Security Policy at minimum)
- Deliver regulatory exposure summary with specific obligations and gap analysis
- Finalize risk register with ownership assignments confirmed with Client

Month 1 Advisory Session

- Conduct first formal monthly advisory session (structured agenda)
- Review 90-day roadmap and confirm priority assignments
- Agree on Q1 deliverables and milestones
- Establish communication protocols and escalation path for incidents

- Confirm board reporting schedule for first quarterly report

30-DAY COMPLETION CHECKLIST — SIGN-OFF

Deliverable	Target Date	Completed	Notes
Technology Sovereignty Risk Assessment delivered	Day 7		
Assessment findings briefing completed	Day 10		
90-Day roadmap delivered	Day 14		
Risk register delivered (initial)	Day 21		
Policy gap analysis completed	Day 21		
Quick wins list actioned (minimum 3 items)	Day 21		
First advisory session completed	Day 30		
Regulatory exposure summary delivered	Day 30		
Board reporting schedule confirmed	Day 30		
Program documentation structure established	Day 30		

Ready to Get Started?

Schedule your complimentary 30-minute discovery call: axiomsovereign.com/consulting
<https://axiomsovereign.com> | axiomsovereign.com