

Virtual CISO Engagement Letter

Scope · Terms · Deliverables · Mutual Obligations

v1.0 — 2026

Virtual CISO Engagement Letter

About This Template

This engagement letter template is used by Axiom Sovereign for all vCISO retainer engagements. It establishes the scope, terms, deliverables, and mutual obligations of the engagement. This template should be reviewed by your legal counsel before execution. Bracketed fields [LIKE THIS] require completion for each specific engagement.

VIRTUAL CISO ENGAGEMENT LETTER

Axiom Sovereign LLC

Severna Park, Maryland · info@axiomsovereign.com · axiomsovereign.com

Date: [ENGAGEMENT DATE]

Client: [CLIENT ORGANIZATION FULL LEGAL NAME]

Client Contact: [PRIMARY CONTACT NAME], [TITLE]

Client Address: [STREET ADDRESS, CITY, STATE, ZIP]

Dear [CONTACT FIRST NAME],

This engagement letter confirms the terms under which Axiom Sovereign LLC ("Axiom Sovereign") will provide Virtual Chief Information Security Officer (vCISO) services to [CLIENT NAME] ("Client"). This letter, together with any attached schedules, constitutes the entire agreement between the parties with respect to the services described herein.

1. SCOPE OF SERVICES

Axiom Sovereign will provide the following services during the term of this engagement:

Service Category	Description	Frequency
Strategic Security Leadership	Serve as Client's virtual CISO, providing executive-level security guidance, program direction, and representation to leadership, board, and third parties including auditors and cyber insurers.	Ongoing
Advisory Sessions	Structured engagement sessions covering program status, risk priorities, regulatory developments, and strategic decisions. Session notes and action items documented after each session.	[FREQUENCY PER MONTH]

Service Category	Description	Frequency
Security Program Development	Design, build, and maintain Client's cybersecurity program including policies, procedures, risk register, vendor management program, and controls framework aligned to [APPLICABLE FRAMEWORK(S)].	Ongoing
Board Reporting	Prepare and deliver quarterly cybersecurity board reports covering risk posture, program status, compliance status, and items requiring board action or decision.	Quarterly
Incident Response Support	Provide first-response advisory support in the event of a suspected or confirmed security incident, including notification requirement guidance and coordination with legal counsel and cyber insurer.	As needed
Regulatory Monitoring	Monitor applicable regulatory developments and update Client on changes with material impact on security or privacy program requirements.	Ongoing
Cyber Insurance Support	Assist with annual cyber insurance renewal questionnaire, carrier communications, and security control evidence documentation.	Annual / as needed

Services NOT included in this engagement unless separately agreed in writing:

- X Penetration testing or vulnerability scanning (may be separately arranged)
- X Software development or IT implementation (controls implementation guidance is included; hands-on implementation of third-party systems may require separate arrangement)
- X Legal counsel, regulatory filings, or representation in enforcement proceedings
- X Managed security services (SOC monitoring, SIEM operation)

2. ENGAGEMENT TIER AND FEES

This engagement is structured under the following tier:

Engagement Tier:	[GOVERNANCE ESSENTIALS / SOVEREIGN ADVISORY / TECHNOLOGY SOVEREIGN]
Monthly Retainer:	[\$AMOUNT] per month, billed on the [1st/15th] of each month
Engagement Period:	[START DATE] through [END DATE] — minimum [6/12] month term
Included Hours:	[X] hours per month. Unused hours do not roll over. Additional hours billed at \$[RATE]/hr.

Setup Fee:	[\$AMOUNT] due upon execution of this letter (one-time)
Renewal:	This engagement automatically renews for successive [6/12]-month periods unless terminated per Section 7.

3. DELIVERABLES

Axiom Sovereign will provide the following written deliverables during the engagement term:

Deliverable	Description	Timing
Onboarding Assessment	Technology Sovereignty Risk Assessment covering AI governance, regulatory exposure, and cybersecurity maturity. Scored baseline with prioritized gap list.	Within 14 days of start date
90-Day Roadmap	Prioritized remediation roadmap for first 90 days of engagement, tied to assessment findings.	Within 21 days of start date
Policy Library	Core security policy documents tailored to Client's industry and regulatory environment. Minimum: Information Security Policy, AI Acceptable Use Policy, Incident Response Plan.	Within 60 days of start date
Risk Register	Initial risk register populated with identified risks, likelihood/impact ratings, current controls, and remediation owners and timelines.	Within 30 days of start date
Quarterly Board Report	Executive-level board report covering security posture, risk status, compliance dashboard, and items requiring board action. See sample report.	Within 10 business days of each quarter end
Annual Program Review	Comprehensive annual review of security program maturity, regulatory compliance posture, and strategic recommendations for the following year.	Annually at engagement anniversary

4. CLIENT RESPONSIBILITIES

Client agrees to provide the following to enable effective delivery of vCISO services:

- Designate a primary point of contact with authority to make or escalate decisions on security matters
- Provide timely access to relevant staff, systems documentation, vendor contracts, and insurance documents
- Respond to requests for information within [5] business days unless otherwise agreed
- Implement or assign implementation of recommendations as agreed in session action items
- Notify Axiom Sovereign promptly of any suspected security incidents, regulatory inquiries, or material changes to Client's technology environment
- Ensure staff participate in required security awareness training and policy acknowledgment processes

5. CONFIDENTIALITY

Both parties agree to maintain the confidentiality of the other party's confidential information. Axiom Sovereign will not disclose Client's confidential business, security, or operational information to third parties without Client's written consent, except as required by law or as necessary to provide the services (e.g., coordinating with legal counsel or incident response vendors during an incident). Client agrees to treat Axiom Sovereign's methodologies, frameworks, and deliverable templates as proprietary and confidential.

6. LIMITATION OF LIABILITY

Axiom Sovereign's total liability for any claim arising under this engagement shall not exceed the total fees paid by Client in the three (3) months preceding the claim. Axiom Sovereign is not liable for: decisions made by Client's leadership based on vCISO recommendations; third-party actions including cyberattacks; regulatory penalties assessed against Client; or any indirect, consequential, or punitive damages. This engagement does not create an attorney-client relationship. Axiom Sovereign is not a law firm and does not provide legal advice.

7. TERM AND TERMINATION

Either party may terminate this engagement with [30/60] days written notice after the minimum term has been completed. During the minimum term, early termination by Client requires payment of the remaining monthly fees for the minimum term. Axiom Sovereign may terminate immediately upon material breach by Client, including non-payment of fees.

8. SIGNATURES

By signing below, both parties agree to the terms of this engagement letter.

AXIOM SOVEREIGN LLC

[CLIENT ORGANIZATION NAME]

Cory Missimore

Founder & Principal Advisor

Date: _____

[AUTHORIZED SIGNATORY NAME]

[TITLE]

Date: _____

Ready to Get Started?

Schedule your complimentary 30-minute discovery call: calendly.com/cmissimore-66kz40min
info@axiomsovereign.com · axiomsovereign.com