Axiom Sovereign

TECHNOLOGY SOVEREIGNTY ADVISORY

VIRTUAL CISO SERVICE — SAMPLE DELIVERABLE

vCISO Quarterly Board Report — Sample

Cybersecurity Program Status · Risk Register · Compliance Dashboard

v1.0 — 2026

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

vCISO Quarterly Cybersecurity Board Report

About This Document

This is a sample Quarterly Cybersecurity Board Report produced by Axiom Sovereign as part of a Virtual CISO engagement. Client-identifying information has been replaced with [CLIENT NAME] and [INDUSTRY] placeholders. Actual engagement reports are tailored to the specific organization, regulatory environment, and risk posture. This sample demonstrates the structure, tone, and depth of board-level reporting you receive as an Axiom Sovereign client.

[CLIENT NAME] — Q2 2026

Cybersecurity Program Status Report · For Board of Directors Review

OVERALL SECURITY POSTURE	RISK TREND	OPEN CRITICAL ISSUES	COMPLIANCE STATUS
MODERATE (Improving)	▲ Improving from Q1	**2 Critical 4 High**	SOC 2: In Progress HIPAA: Compliant Cyber Ins: Renewed

EXECUTIVE SUMMARY

This report covers cybersecurity program activities for Q2 2026 (April 1 – June 30, 2026). The overall security posture of [CLIENT NAME] has improved from Q1, driven by the successful deployment of multi-factor authentication across all staff accounts and the completion of the annual HIPAA Security Risk Analysis. Two critical-priority issues remain open and require board awareness: the absence of a tested incident response plan and unresolved vendor contracts lacking security requirements. Both are on track for remediation in Q3 2026.

No security incidents were reported during Q2. One near-miss event — a staff member entering client tax data into an unapproved AI tool — was identified through the new DLP monitoring system, addressed through coaching, and documented as a program improvement event. This demonstrates the effectiveness of recently deployed controls.

PROGRAM HIGHLIGHTS — Q2 2026

Initiative	Status	Business Impact	Owner
MFA Deployment — All 47 staff accounts	COMPLETE	Eliminates #1 ransomware and BEC attack vector. Reduces cyber insurance premium ~12% at next renewal.	IT / vCISO

Initiative	Status	Business Impact	Owner
HIPAA Security Risk Analysis	COMPLETE	Satisfies mandatory annual requirement (45 CFR §164.308(a)(1)). Avoids $100K–$1.9M potential OCR penalty exposure.	vCISO
AI Acceptable Use Policy — Deployment	COMPLETE	100% staff acknowledgment received. Addresses AICPA ET 1.700 compliance gap identified in Q1 assessment.	vCISO / HR
DLP Monitoring — Microsoft 365 Purview	COMPLETE	Detects and alerts on sensitive data (SSNs, PHI) transmissions to external services. 1 near-miss identified Q2.	IT / vCISO
Incident Response Plan — Development	IN PROGRESS (Q3 Target)	Required for cyber insurance compliance and HIPAA breach response. Tabletop exercise planned Q3.	vCISO / Legal
Vendor Security Contracts — Review	IN PROGRESS (Q3 Target)	Addresses third-party risk gap. Priority: EHR vendor, billing service, and cloud storage contracts.	vCISO / Operations

TOP RISKS — CURRENT STATUS

Risk	Severity	Current Controls	Residual Risk	Remediation & Timeline
No tested incident response plan. Staff are unaware of notification obligations under HIPAA (60-day) and state breach laws.	CRITICAL	Basic IT recovery procedures exist. No documented IR plan.	HIGH — A breach today would result in missed notification deadlines and OCR exposure.	IR plan draft complete by Aug 15. Tabletop exercise Sept 2026. Board approval requested Q3.
Vendor contracts lacking security requirements and breach notification clauses.	CRITICAL	BAAs in place for EHR vendor. Billing service and cloud storage lack security terms.	HIGH — Third-party breach with client data would trigger regulatory exposure and potential client liability.	vCISO conducting vendor review. Priority contracts (2) to be updated by Sept 30, 2026.
Security awareness training not completed — 6 of 47 staff pending.	HIGH	Training deployed to 41 staff (87% completion). Non-completion tracked.	MODERATE — Incomplete training creates phishing vulnerability and insurance compliance gap.	Manager escalation in progress. 100% completion required by July 31, 2026.
Endpoint patching — 3 workstations running outdated Windows versions.	HIGH	Automatic updates enabled for most systems. 3 exceptions documented.	MODERATE — Known vulnerabilities on outdated endpoints. Low probability, high impact.	IT scheduled updates for July 2026. One system flagged for hardware replacement.
No formal backup restoration testing.	MODERATE	Daily backups running to Azure. Offsite copy enabled. Never tested.	MODERATE — Untested backups may fail during ransomware recovery.	Restoration test scheduled Q3. Will document result and report Q3 board report.

COMPLIANCE DASHBOARD

Framework / Requirement	Status	Key Gap	Next Milestone
HIPAA Security Rule (45 CFR 164)	COMPLIANT	Incident Response Plan pending	IR Plan: Aug 2026
Cyber Insurance — Carrier Controls	COMPLIANT	Restoration testing not yet performed	Backup test: Q3 2026

Framework / Requirement	Status	Key Gap	Next Milestone
AICPA ET Section 1.700 (AI Governance)	COMPLIANT	Ongoing monitoring required	Quarterly policy review
SOC 2 Type II Readiness	IN PROGRESS	Multiple controls under development	Readiness assessment: Q4 2026
State Privacy Laws (applicable jurisdictions)	COMPLIANT	Annual DSAR log review due	Annual review: Dec 2026

ITEMS REQUIRING BOARD ACTION

Board Decision Required

1. Incident Response Plan — Approval Required (Q3 2026)

The vCISO will present the completed Incident Response Plan to the board for approval in Q3. The plan designates board-level notification responsibilities and authorizes engagement of the IR retainer firm ($15,000 annual retainer). Board approval is required to execute the retainer.

2. Security Awareness Training Budget — FY2027 Planning

Current training is delivered via the vCISO engagement. For FY2027, Axiom Sovereign recommends a dedicated phishing simulation and awareness training platform ($1,800–$2,400/year for 47 staff). Board awareness requested; formal budget request will be submitted with FY2027 budget.

Ready to Get Started?

Schedule your complimentary 30-minute discovery call: calendly.com/cmissmore-62kc/30min
info@axiomsovereign.com · axiomsovereign.com