Axiom Sovereign

TECHNOLOGY SOVEREIGNTY ADVISORY

CFO'S DECISION GUIDE

The vCISO vs. Full-Time CISO Decision

Economic Analysis · Decision Framework · ROI Calculator

v1.0 — 2026

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

The vCISO vs. Full-Time CISO Decision: A CFO's Guide

About This Guide

This guide provides financial decision-makers — CFOs, managing partners, and executive directors — with the analytical framework to evaluate whether a full-time Chief Information Security Officer or a fractional Virtual CISO (vCISO) is the right security leadership model for their organization. It includes a complete total cost of ownership analysis, a capability comparison matrix, a decision framework based on organizational characteristics, and an ROI calculation tool.

The decision between full-time and fractional security leadership is not primarily a security decision — it is a financial and operational decision. Most mid-market organizations are better served by a well-structured fractional engagement than a full-time hire, not because fractional is cheaper, but because a senior fractional practitioner with broad cross-industry experience typically delivers more relevant expertise than a full-time hire at the same cost level. This guide helps you reach that conclusion — or challenge it — with real data.

The Core Question

Can you get 80–90% of the value of a full-time CISO at 10–20% of the cost? For most organizations under 500 employees, the answer is yes — but only if the vCISO engagement is structured correctly. This guide tells you what to look for and what to avoid.

How to Use This Guide

Read this guide in three stages: First, review the total cost analysis to establish an accurate baseline for what a full-time hire actually costs. Second, use the decision framework to evaluate your organization's profile against the key indicators for each model. Third, complete the ROI calculator with your organization's specific numbers to quantify the financial case.

PART 1: THE REAL COST OF A FULL-TIME CISO

Most organizations significantly underestimate the total cost of a full-time CISO hire. The base salary is the most visible cost — but it typically represents only 55–65% of the true total cost. The following table presents a complete cost model based on U.S. market data for CISOs in mid-market organizations.

Cost Component	Low Estimate	Mid Estimate	High Estimate	Notes
Base Salary	$180,000	$230,000	$320,000	Varies by market, industry, experience
Bonus (15–25% of base)	$27,000	$46,000	$80,000	Standard for VP/C-level roles
Benefits (healthcare, dental, vision, 401K)	$36,000	$55,000	$96,000	20–30% of base salary
Equity / Long-Term Incentives	$15,000	$40,000	$100,000	RSUs, options, or profit share
Payroll Taxes (FICA, FUTA, SUTA)	$15,000	$19,000	$26,000	~8% of base salary
Recruiting / Executive Search Fee	$36,000	$55,000	$96,000	20–30% of first-year comp
Onboarding & Ramp Time (3–6 months)	$45,000	$72,500	$120,000	Partially productive during ramp
Tools, Training, Conferences	$15,000	$25,000	$40,000	GRC platform, certifications, travel
Office Space / Equipment	$8,000	$12,000	$20,000	For in-office or hybrid roles
TOTAL — YEAR ONE	$377,000	$554,500	$898,000	Full loaded cost including recruiting
ONGOING ANNUAL COST (Year 2+)	$296,000	$427,000	$738,000	Excluding recruiting and onboarding

These numbers have important implications. A mid-market organization that hires a CISO at $230,000 base salary is committing to approximately $554,500 in Year 1 costs and $427,000 annually thereafter — before any tools, infrastructure, or additional security staff. For most organizations under 500 employees, this represents a security budget commitment that absorbs the entire security function budget for other purposes.

PART 2: THE VCISO MODEL — ECONOMICS AND CAPABILITY

A fractional vCISO engagement provides security leadership on a defined monthly retainer basis. The practitioner functions as your CISO for the scope of the engagement — attending board meetings, leading your security program, managing incidents, and interfacing with auditors and insurers — but at a fraction of the full-time cost. The following table compares engagement tier economics against the full-time alternative.

Engagement Tier	Monthly Retainer	Annual Cost	Hours / Month	Best Fit Organization
Governance Essentials (Starter)	$3,500–$5,000	$42,000–$60,000	8–12 hours	Under 50 employees. No prior security program. Cyber insurance compliance is primary driver.
Sovereign Advisory (Growth — Most Popular)	$6,500–$9,000	$78,000–$108,000	20–28 hours	25–200 employees. Active compliance requirement (SOC 2, HIPAA, client contracts). Program build needed.
Technology Sovereign (Enterprise)	$12,000–$18,000	$144,000–$216,000	40–60 hours	100–500 employees. Complex regulatory environment. Government contracts. Multi-framework compliance.
Full-Time CISO (Reference)	$21,500–$49,700+	$258,000–$596,000+	160+ hours	500+ employees. Dedicated security team to manage. Critical infrastructure or classified data.

Key insight: The Sovereign Advisory tier at $6,500–$9,000/month ($78,000–$108,000 annually) provides 20–28 hours per month of senior CISO-level attention — comparable to 25–35% of a full-time CISO's time, at 20–30% of the cost. For most mid-market organizations, this is the economically rational choice.

PART 3: DECISION FRAMEWORK — WHICH MODEL IS RIGHT FOR YOU?

Use the following framework to evaluate which security leadership model matches your organization's profile. The indicators in each column represent the organizational characteristics most strongly correlated with each model's success.

Organizational Factor	Indicators for Full-Time CISO	Indicators for vCISO
Employee Count	500+ employees	Under 500 employees — especially under 200
Dedicated Security Staff	Managing a team of 5+ security analysts or engineers	No dedicated security staff, or 1–2 staff needing leadership
Annual Security Budget	$2M+ dedicated to security tools, staff, and operations	Under $500K total security spend

Organizational Factor	Indicators for Full-Time CISO	Indicators for vCISO
Regulatory Complexity	Multiple complex frameworks with frequent third-party audits (FedRAMP, HITRUST, PCI DSS Level 1)	Standard compliance requirements (SOC 2, HIPAA, NIST CSF, GDPR)
Data Sensitivity Level	Critical infrastructure, classified data (CUI/SCI), national security systems	Standard PII, protected health information, client financial and legal data
Board Engagement	CISO presents to board monthly or more frequently	Quarterly board presentation or as-needed reporting
Technology Complexity	100+ enterprise applications, hybrid cloud spanning multiple hyperscalers, OT/ICS environments	Standard Microsoft 365 or Google Workspace, 1–2 cloud environments
Geographic Scope	Global operations across 10+ countries with complex data sovereignty requirements	U.S.-focused operations or limited international presence
M&A; Activity	Frequent acquisitions requiring security integration and due diligence at scale	Stable organizational structure
Verdict	Most organizations that believe they need a full-time CISO discover they needed a senior vCISO when they benchmark against these criteria.	Most mid-market professional services organizations are best served by a fractional engagement at the Sovereign Advisory tier or above.

PART 4: WHAT TO LOOK FOR — AND WHAT TO AVOID — IN A VCISO

Not all vCISO engagements are equal. The market has a significant quantity of providers who market vCISO services but deliver junior-consultant execution or advisory-only relationships that leave clients responsible for implementing everything themselves. The following criteria help you evaluate and distinguish genuine vCISO engagements.

What a high-quality vCISO engagement delivers:

- Named senior practitioner — you know exactly who your vCISO is, they know your organization, and they are consistently available to you
- Executive credibility — can represent your security program to your board, external auditors, cyber insurers, and enterprise clients without qualification
- Hands-on execution — authors policies, configures controls, manages vendors, and delivers documentation — not just provides recommendations
- Incident response capability — available and accountable when an incident occurs, not just during scheduled advisory sessions
- Regulatory competence specific to your industry — a vCISO who cannot interpret AICPA ethics guidance or HIPAA requirements cannot serve a professional services firm effectively

Red flags that indicate a low-quality vCISO engagement:

- Junior staff marketed as "vCISO" — ask for the named practitioner's credentials, not the firm's resume
- Team-based model with rotating staff — if different people show up each engagement, your vCISO does not know your organization
- Advisory-only delivery — if you still have to implement everything yourself, you hired a consultant, not a CISO
- No board reporting capability — ask to see a sample board presentation before you sign
- Framework deliverables as the primary output — a 300-page NIST CSF report that sits on a shelf is not a security program
- Offshore or AI-only delivery — regulatory interpretation, professional accountability, and incident response require a human practitioner who can be held responsible
- Tool-dependent model — "you must purchase our GRC platform" as a condition of engagement creates vendor lock-in and misaligned incentives

PART 5: ROI CALCULATOR

Complete the following with your organization's actual numbers to quantify the financial case for your security leadership decision.

Full-Time CISO Cost Analysis

Estimated base salary for CISO at our organization's size and location: $_____

Total benefits and payroll taxes (add 28–35% of base): $_____

Recruiting / search firm cost (add 20–30% of base, Year 1 only): $_____

Tools, training, conferences (estimated): $_____

TOTAL YEAR 1 FULL-TIME COST: $_____

ONGOING ANNUAL COST (Year 2+): $_____

vCISO Comparison

Selected vCISO tier (circle one): Governance Essentials / Sovereign Advisory / Technology Sovereign

Monthly retainer: $_____ Annual cost: $_____

Financial Analysis

Year 1 savings (Full-Time Year 1 cost minus vCISO annual cost): $_____

Ongoing annual savings (Full-Time Year 2+ cost minus vCISO annual cost): $_____

3-Year cumulative savings: $_____

5-Year cumulative savings: $_____

Next Step

Axiom Sovereign engagements mobilize within 5 business days of a signed agreement. The initial Technology Sovereignty Risk Assessment is typically delivered within 2 weeks of kickoff. Schedule a complimentary 30-minute discovery call to discuss your organization's profile, receive a recommended engagement tier, and ask any questions about the vCISO model.

Book at: calendly.com/cmissimore-6zkc/30min

Email: info@axiomsovereign.com · **Web:** axiomsovereign.com