

Hudson Infosec®

vCISO Partner Guide

From IT Leader to vCISO

A practical launch guide for senior IT professionals stepping into virtual CISO consulting.

Why vertical specialization wins. How to price and package services. And the operational stack that lets you scale without becoming a system integrator.

Published by Hudson Infosec, LLC for prospective partners in the Hudson Infosec vCISO Program.

Contents

Foreword A note for the recently displaced 3

Part I The vCISO Opportunity

1 What a vCISO actually does 4

2 Why the market exists — and why now 5

3 From IT leader to security advisor 7

Part II Pick Your Lane

4 Why generalists lose 9

5 Healthcare 11

6 Legal 13

7 Manufacturing 15

8 Defense Industrial Base (DoD / CMMC) 17

9 Financial services & credit unions 19

10 Education (K-12 and higher ed) 21

Part III Building the Practice

11 Your service catalog 22

12 Pricing your engagements 24

13 Credentials worth chasing 25

Part IV The Operational Stack

14 The infrastructure problem 27

15 The Hudson Infosec vCISO Program 28

16 Mapping the platform to each vertical 30

Part V Execution

17 Your first 90 days 32

18 Pitfalls, and how to avoid them 34

19 Next steps 35

FOREWORD

A note for the recently displaced

If you are reading this within a few weeks of an unexpected job change, first: the timing is not as bad as it feels. The cybersecurity advisory market has a chronic shortage of seasoned operators. There are roughly 700,000 unfilled cyber roles in the United States. Cyber-insurance underwriters are demanding documented CISO oversight from companies that have never had one. Regulators in healthcare, defense contracting, financial services, and education are tightening reporting requirements every quarter. Small and mid-sized firms in these industries cannot recruit a full-time CISO at $250,000+ — but they are required, by contract or by regulation, to have one. That gap is the vCISO market.

Second: the skills you spent twenty or thirty years building — running infrastructure, leading IT teams, surviving audits, negotiating with vendors, explaining technical risk to non-technical executives — are the same skills this market is paying for. You do not need to retool. You need to repackage.

This guide is the playbook we wish someone had handed us when we started. It is opinionated. It tells you to specialize early. It explains how vCISOs actually make money (it is not what most newcomers think). It walks through the regulatory landscape of each major vertical at enough depth to let you decide where to plant your flag. And it is honest about the operational trap that kills most new advisory firms in their second year: you cannot scale a consulting practice if you are personally running every vulnerability scan, writing every report, and stitching together five separate vendor portals for each client. That is what the back half of this guide addresses.

ABOUT THE PUBLISHER

Hudson Infosec is a cybersecurity firm based in Poughkeepsie, NY, building operational infrastructure for vCISO consultancies and regulated-industry clients. Our vCISO Partner Program — described in Part IV — is the white-label stack that powers many of the practices founded by readers of this guide. The first three parts of this document, however, are vendor-neutral career guidance. Treat them as the starting point; treat Part IV as one specific answer to the operational question.

PART I — CHAPTER 1

What a vCISO actually does

A virtual Chief Information Security Officer is a fractional executive. You are hired by an organization that needs CISO-level judgment — strategy, risk prioritization, board reporting, regulatory liaison — but cannot justify the cost of a full-time hire. Typical client size is 50 to 500 employees, with annual revenues from $10 million to $250 million, operating in an industry where some form of cybersecurity oversight is contractually or legally required.

The day-to-day work breaks into four buckets. Understanding these buckets matters because each one has a different billing model and a different delivery rhythm.

Strategic advisory

Quarterly business reviews with the CEO or board. Multi-year roadmaps. Mergers-and-acquisitions diligence. Vendor risk reviews on major contracts. This is the visible, billable-at-premium-rate work — usually a flat monthly retainer of $4,000 to $15,000 depending on client size.

Governance and compliance

Writing and maintaining the security program: policies, procedures, the incident response plan, the disaster recovery plan, the business continuity plan. Mapping controls to whichever framework the client must demonstrate compliance with — HIPAA, NIST SP 800-171, CMMC, SOC 2, ISO 27001, PCI DSS, GLBA, FERPA. Running tabletop exercises. Preparing for and sitting through audits. This work is typically bundled into the retainer.

Operational oversight

Reviewing scan results, threat intelligence, security event logs, and incident reports. Authorizing patches. Approving exception requests. Coordinating with the client's IT team or their managed service provider. This is where new vCISOs often drown — it is high-volume, low-leverage work unless you have tooling that pre-processes the noise. Part IV addresses this directly.

Project and incident work

Risk assessments, penetration testing engagements, vendor selection projects, and — eventually — actual incident response. This is billed on top of the retainer, usually as fixed-fee projects or as time-and-materials engagements with a not-to-exceed cap.

> **RULE OF THUMB**
>
> A healthy vCISO practice earns roughly 60% of revenue from retainers, 30% from project work, and 10% from incident response and emergency engagements. If your retainer share drops below 50%, you are running a consulting shop, not an advisory practice. The economics are different and the burnout rate is higher.

PART I — CHAPTER 2

Why the market exists — and why now

Three structural forces are driving demand for fractional CISO services. Each of them has been building for years; together they have produced the current shortage.

The talent gap

There are not enough qualified senior security leaders to staff the demand. The cybersecurity workforce gap in the United States is estimated at around 500,000 to 700,000 unfilled roles depending on which annual survey you read. At the CISO level specifically, the median compensation in metro markets is over $300,000 fully loaded — out of reach for any company below roughly $100 million in revenue. The math forces fractional models.

Regulatory expansion

Five years ago, only finance, healthcare, and defense contractors faced binding cybersecurity regulation. Today the perimeter is much wider. The SEC requires public companies to disclose material cyber incidents on Form 8-K within four business days, with annual narrative disclosure of governance and risk management practices. State privacy laws now blanket most of the U.S. consumer market. CMMC 2.0 is in active rollout for the defense industrial base. The FTC Safeguards Rule applies to a broad class of financial-data handlers including many companies that do not think of themselves as financial services. HIPAA enforcement actions have moved downstream to small medical practices and their business associates. The common theme: organizations that previously had no compliance officer now need one, and they need them quickly.

Cyber-insurance underwriting

Even where regulation does not require a CISO, insurance underwriters increasingly do. Coalition, At-Bay, Resilience, Beazley, AXIS — the major cyber carriers have substantially tightened their underwriting questionnaires over the past two renewal cycles. Multi-factor authentication, documented incident response plans, regular penetration testing, EDR deployment, and named executive accountability for security are now standard prerequisites for coverage at meaningful policy limits. A vCISO retainer is a cheap way to check those boxes — and, in some carrier programs, qualifies for a premium discount.

> **THE TAM, SIZED ROUGHLY**
>
> Industry analysts (Forrester, Gartner) place the U.S. vCISO services market at $2 to $4 billion in 2025, with growth in the 25% to 35% annual range. Estimated U.S. vCISO firm count is in the low thousands, from solo practitioners through 50-plus person consultancies. The market is fragmented enough that a new entrant with a focused vertical specialization can build a sustainable book of business within twelve to eighteen months.

Why now?

The convergence of these three forces is recent. Pre-pandemic, the demand was real but the buyers were slow. The combination of ransomware events in 2020 to 2023, the SolarWinds and Kaseya supply-chain incidents, executive orders on federal cybersecurity, the SEC disclosure rules taking effect in late 2023, and the CMMC 2.0 final rule have moved cybersecurity from a recommended best practice to a contractual line item. Buyers who deliberated for a year now sign engagement letters in three weeks.

If you are entering this market in 2026, you are doing so at a moment when demand exceeds supply, prices are firm, and customer expectations are shaped enough that you can sell standard packages rather than bespoke engagements for every prospect. This was not true five years ago.

PART I — CHAPTER 3

From IT leader to security advisor

The transition from senior IT operator to vCISO is shorter than most people assume — but it is not zero. Three shifts matter.

Shift one: from execution to oversight

As an IT director, your value came from making things work. As a vCISO, your value comes from deciding what should be done, by whom, and verifying that it has been done. Most newcomers struggle with this in the first six months. They keep wanting to fix the firewall rule themselves. The discipline of writing a recommendation, handing it to the client's IT team, and following up at the next review takes practice.

Why this matters operationally: your hourly rate as an advisor is two to three times what it would be as an operator. Every hour you spend configuring infrastructure is an hour you are not selling at advisor rates — and an hour that the client is not learning to do without you. Done well, a vCISO engagement should make the client less dependent on you over time, not more. That is what produces referrals.

Shift two: from technical to translational

CEOs, boards, regulators, and insurance brokers do not want to hear about CVSS scores or attack vectors. They want to know what the risk means to their business in dollars and reputational terms, what it would cost to fix, and whether they should accept it. The vCISOs who command the highest rates are the ones who can write a one-page board memo that translates a vulnerability scan into a business decision.

This is a learnable skill, but it requires deliberate practice. Many new vCISOs benefit from drafting their first three or four executive memos against a template and having a peer review them. Once the pattern clicks, every report you produce thereafter compounds in value, because it doubles as marketing collateral when the client shares it with their board, their lawyer, their auditor, or their insurer.

Shift three: from employee to founder

This is the hardest shift. You are now responsible for sales, contracting, billing, professional liability insurance, your own benefits, and your own marketing. Most senior IT leaders have never sold anything. The good news is that the vCISO sales motion is the most consultative of any professional service category — buyers want a relationship, not a pitch. Your sales advantage is your decades of credibility. Your weakness is that you may not be comfortable asking for the business directly.

Practical recommendations for the first ninety days:

- Form an LLC in your home state. A single-member LLC taxed as an S-corp is the most common structure for solo vCISO practices and minimizes self-employment tax once you cross roughly $80,000 in net income.
- Get professional liability and cyber liability insurance before signing your first engagement letter. Expect to pay $2,000 to $5,000 annually for $1M / $1M coverage from carriers like Hiscox, The Hartford, or specialty cyber underwriters.

- Open a separate business bank account and a separate credit card. The bookkeeping friction of mingled accounts will eat ten hours a month you cannot afford.
- Build a one-page services description and a standard engagement letter. Have an attorney familiar with consulting agreements review them once. After that, reuse them.
- Pick your vertical (Part II). Do not skip this step. The cost of being a generalist in your first year is far higher than any specialization you might regret later.

ON IMPOSTER SYNDROME

Almost every new vCISO feels underqualified. Almost every new vCISO is, in fact, qualified — they simply have not yet adjusted to charging for what they used to do as part of a salary. If you spent fifteen years running infrastructure for a hospital, you know more about healthcare security operations than 90% of the consultants currently billing for it. The credential is helpful (Part III, Chapter 13). The track record is what closes the deal.

PART II — CHAPTER 4

Why generalists lose

Every new vCISO faces the same temptation: take whatever client walks in the door, because revenue is revenue. This is the single most expensive mistake in the early years of an advisory practice. The economics of generalism are bad, and the economics get worse the longer you stay general.

Here is why.

Time. Every regulated industry has its own framework, its own auditor behavior, its own vocabulary. Walking into a HIPAA engagement cold and walking into a CMMC engagement cold are not the same exercise even if the underlying controls overlap by 70%. The 30% that differs — documentation conventions, scoping methodology, evidence formats — consumes weeks of unbilled study per new vertical. A generalist serving four industries pays this tax four times. A specialist pays it once.

Pricing. Specialists charge more. A vCISO who is known as the person for ophthalmology practices in the Northeast prices their healthcare engagements 20% to 40% higher than a generalist competing for the same client. The client pays the premium because they perceive — correctly — that the specialist will produce a better outcome with less hand-holding. Premium pricing in your specialty subsidizes the rest of your business.

Referrals. Vertical specialists get vertical referrals. A managed service provider serving credit unions, an attorney who handles healthcare M&A, an insurance broker writing manufacturing policies — these are the referral sources that produce a steady book of business. They refer to the person they already think of as their industry's vCISO. They do not refer to a generalist, because they have no way of explaining the generalist's value to the next prospect.

The trap of "I'll just take this one client"

In year one, every prospect looks attractive. A first-year vCISO often ends up with one healthcare client, one law firm, one manufacturer, and one credit union. Six months in, this practice is unsustainable. Each client requires a different framework, different reporting templates, different audit cycles, different language in board presentations. The practice cannot grow because every new client adds linear overhead.

The fix is to pick a vertical before you have your first client and to decline engagements outside it, politely, even when offered. Yes, this feels counterintuitive. It also works. The next six chapters describe the six verticals where there is currently the most pull. Read all of them. Pick one — at most two adjacent ones.

HOW TO CHOOSE

Pick the vertical where (a) you have prior employment or domain experience, (b) there are at least 200 prospective client organizations within your geographic reach, and (c) the regulatory or insurance pressure is strong enough that buyers are actively shopping. If you can answer yes to all three for one industry, that is your lane. If two industries tie, pick the one with the higher average engagement size.

PART II — CHAPTER 5

Healthcare

Healthcare is the largest and most fragmented vertical in the vCISO market. It contains everything from one-physician dental practices to multi-state hospital systems, with regulatory exposure that has tightened sharply since the HHS Office for Civil Rights began publishing enforcement settlements at current scale.

The regulatory landscape

HIPAA is the foundation: the Privacy Rule (45 CFR Part 160 and Subparts A and E of Part 164), the Security Rule (Subpart C of Part 164), and the Breach Notification Rule (Subpart D). HITECH amended HIPAA in 2009 to add breach notification, increased penalties, and direct enforcement against Business Associates. State laws layer on top — California's CMIA, Texas HB 300, New York's SHIELD Act for protected health information held by NY entities. Some health plans also fall under GLBA for the financial components of their operations.

In practice, a healthcare client cares about three documents: the Risk Analysis (HIPAA Security Rule §164.308(a)(1)(ii)(A)), the Risk Management Plan that follows from it, and evidence of ongoing monitoring. If you can produce these three artifacts to the standard an OCR investigator would accept, you are 80% of the way to a defensible HIPAA posture for a small or mid-sized covered entity. The remaining 20% is workforce training, Business Associate Agreement management, and incident response readiness.

Buyer profile and engagement structure

Small medical practices — under 25 providers — typically buy a one-time Risk Analysis ($8,000 to $20,000) followed by a monthly retainer of $2,000 to $4,500 for ongoing oversight. Mid-sized practices and small hospital systems pay retainers of $5,000 to $12,000 monthly and budget annual penetration testing of $15,000 to $40,000. Business Associates — particularly billing companies, claims clearinghouses, transcription services, and medical device vendors — are an underserved sub-segment that often has more sophisticated needs than the covered entities themselves but smaller budgets.

Sub-segment	Typical retainer	Annual project budget
Small practice (1-25 providers)	$2,000 – $4,500 / month	$10,000 – $30,000
Mid-size practice / clinic group	$5,000 – $9,000 / month	$25,000 – $75,000
Small hospital / health system	$8,000 – $15,000 / month	$50,000 – $200,000
Business Associate (billing, clearinghouse)	$3,000 – $7,000 / month	$15,000 – $60,000

Sub-segment	Typical retainer	Annual project budget
Medical device or HealthTech vendor	$5,000 – $12,000 / month	$40,000 – $150,000

Where to find clients

Healthcare buyers are organized through professional associations and specialty societies. Medical Group Management Association (MGMA) chapters, state medical societies, hospital associations, and regional Healthcare Information and Management Systems Society (HIMSS) chapters are the most productive channels. Healthcare-focused MSPs and EHR resellers also refer frequently — many of them do not want to take HIPAA responsibility themselves and welcome a named vCISO they can point at when clients ask.

> **HEALTHCARE GOTCHA**
>
> Do not promise HIPAA compliance. HIPAA does not have a compliance certification, and any vendor or consultant who claims to certify it is selling snake oil. What you deliver is a defensible posture, documented, with the artifacts an OCR investigator or a Business Associate's auditor would expect to see. Set this expectation in your engagement letter and your marketing copy. Sophisticated buyers will respect the precision; unsophisticated ones will need to be educated.

PART II — CHAPTER 6

Legal

Law firms are a small but high-margin vertical. The buyer is sophisticated, the rates are firm, and the work compounds because firms refer to each other within their specialty bars.

The regulatory landscape

Law firms are not regulated by an agency in the same way healthcare or defense contractors are. They are regulated by their professional duties. ABA Model Rule 1.6(c) requires lawyers to make reasonable efforts to prevent the unauthorized disclosure of client information; ABA Formal Opinions 477R (2017) and 483 (2018) interpret this as requiring active cybersecurity competence and incident response capability. State bar rules adopt or modify these requirements with local variations.

On top of professional rules, firms are subject to the regulatory exposure of their clients. A law firm representing healthcare entities handles protected health information as a Business Associate. A firm representing defense contractors handles controlled unclassified information. A firm doing financial services work handles non-public personal information under GLBA. Outside counsel guidelines — the security requirements that corporate clients impose on the firms they hire — have become detailed enough that compliance with them is the practical security baseline.

Buyer profile and engagement structure

Small firms (under 25 lawyers) typically engage a vCISO after a security incident, after losing a request for proposal because they could not meet client security requirements, or after their malpractice carrier raises the question. Engagement starts with a current-state assessment and a policy program: written information security plan, incident response plan, acceptable use policy, vendor management procedure. Followed by a retainer for ongoing oversight, response to client security questionnaires, and annual penetration testing.

Mid-sized firms (25 to 250 lawyers) often have an IT director already and are looking for advisory oversight rather than execution. The retainer is smaller but the project pipeline — annual penetration testing, tabletop exercises, vendor diligence on the firm's litigation support vendors and e-discovery providers — is steady.

Firm size	Typical retainer	Annual project budget
Solo / small (1-10 lawyers)	$1,500 – $3,500 / month	$8,000 – $25,000
Mid-small (10-50 lawyers)	$3,500 – $7,500 / month	$25,000 – $80,000
Mid-size (50-250 lawyers)	$6,000 – $12,000 / month	$60,000 – $200,000
Practice-specialty boutique	$3,000 – $8,000 / month	$30,000 – $120,000

Where to find clients

State and local bar associations have technology committees that book speakers. The International Legal Technology Association (ILTA) publishes the LegalSEC Risk and Compliance reference and runs an annual conference. Legal-focused MSPs are an excellent referral channel — many of them have an internal SOC but no named CISO to point at when clients ask. Outside counsel security questionnaires from major corporate clients are a forcing event: firms that fail one questionnaire often issue an engagement letter within thirty days.

PART II — CHAPTER 7

Manufacturing

Manufacturing is the vertical most often underestimated by new vCISOs. The buyers are unsophisticated by metropolitan standards — many are second or third generation owners running operations their grandfathers founded — but the exposure is significant, the supply-chain pressure is rising, and the engagement sizes can be substantial when industrial control systems are involved.

The regulatory and contractual landscape

Pure-play domestic manufacturers without defense or healthcare exposure face limited direct regulation. What drives demand is supply-chain pressure: their large customers — automotive OEMs, aerospace primes, medical device OEMs, retailers — are imposing cybersecurity requirements on suppliers as a condition of doing business. The Automotive Industry Action Group (TISAX in Europe, evolving practices in North America), aerospace primes cascading NIST SP 800-171 to subcontractors, and retailer security questionnaires all create indirect compliance obligations that the manufacturer typically discovers through a single sentence in a contract amendment.

Manufacturers that touch defense contracting, even at low tiers, fall under DFARS 252.204-7012 and the cascading CMMC requirements covered in Chapter 8. Manufacturers that handle personal data — most do, through their HR and customer systems — fall under state privacy laws.

OT/IT convergence

The differentiator in manufacturing is operational technology: the programmable logic controllers, human-machine interfaces, historians, and SCADA systems that run the factory floor. These systems were designed in eras when network connectivity was rare, security was assumed, and patching was something done during scheduled downtime years apart. They now sit on networks reachable from corporate IT, often without segmentation.

A vCISO serving manufacturing needs at least a working understanding of OT protocols — Modbus, DNP3, EtherNet/IP, OPC UA, IEC 60870-5-104 — and the operating philosophies that distinguish IT from OT (availability and safety dominate confidentiality; downtime to patch is rarely acceptable; vendor-controlled HMIs cannot be modified). You do not need to be an industrial controls engineer. You do need to understand why the controls engineer is going to push back on every change you propose, and how to find the compromises that work.

Sub-segment	Typical retainer	Annual project budget
Small job shop / contract manuf.	$2,500 – $5,000 / month	$15,000 – $50,000
Mid-size discrete manufacturer	$5,000 – $10,000 / month	$40,000 – $150,000
Process / chemical / food manuf.	$6,000 – $12,000 / month	$60,000 – $250,000

Sub-segment	Typical retainer	Annual project budget
Tier 2 or 3 defense supplier	$8,000 – $15,000 / month	$80,000 – $350,000

Where to find clients

Manufacturing extension partnerships (the MEP network funded by NIST and operating in every state), regional manufacturing associations, and industry-specific groups like the Precision Machined Products Association are productive. Insurance brokers writing manufacturing risk are an underused channel. Local economic development authorities often introduce vCISOs to companies pursuing growth grants that have cybersecurity attestations as application requirements.

MANUFACTURING ENTRY TACTIC

The single most reliable way to enter manufacturing is to develop a named relationship with one or two large OEMs in your region whose supply chains include small manufacturers. The OEM does not pay you. But when the OEM sends out an annual security attestation request to its suppliers, the suppliers — panicked — look for help. A vCISO who is on the OEM's recommended-or-known list gets the call. This is how automotive-supply-chain vCISO practices in Michigan and Ohio were built; it works in any industrial cluster.

PART II — CHAPTER 8

Defense Industrial Base (DoD / CMMC)

The Defense Industrial Base is the most lucrative single vertical for new vCISOs entering the market in 2026, and the one with the steepest learning curve. Roughly 220,000 organizations contract with the Department of Defense, the vast majority of them small and mid-sized. Every one of them is now staring down CMMC 2.0.

The CMMC 2.0 framework

The Cybersecurity Maturity Model Certification, version 2.0, is the Department of Defense's program for verifying that contractors and subcontractors implement the cybersecurity controls required by DFARS 252.204-7012 and NIST SP 800-171. The final rule was published in late 2024 (32 CFR Part 170), with the contractual flow-down rule (48 CFR / DFARS) taking effect in phased implementation through 2025 to 2028.

CMMC defines three levels:

- **Level 1** covers Federal Contract Information (FCI). Fifteen basic safeguarding requirements drawn from FAR clause 52.204-21. Annual self-assessment with senior official affirmation.
- **Level 2** covers Controlled Unclassified Information (CUI). The 110 controls of NIST SP 800-171 Revision 2 (transitioning to Revision 3). For most CUI contracts, third-party certification by a CMMC Third-Party Assessment Organization (C3PAO) every three years.
- **Level 3** covers the most sensitive CUI, including programs of particular criticality. NIST SP 800-171 plus selected enhancements from NIST SP 800-172. Government-led assessment by DCMA's DIBCAC.

In practice, more than 80,000 organizations will need Level 2 certification. The supply of qualified C3PAO assessors is constrained. Demand for vCISO support — both for the certification preparation work and for the post-certification continuous monitoring required to maintain the posture — is durable for at least the next decade.

Engagement structure

CMMC engagements have a distinct shape that differs from other verticals. A typical sequence:

- **Scoping and gap assessment.** Define the CUI environment. Map people, processes, facilities, and information systems against NIST SP 800-171 controls. Produce a current System Security Plan (SSP) and a Plan of Action and Milestones (POA&M). Six to twelve weeks. $20,000 to $60,000 fixed fee.
- **Remediation.** Close the gaps identified in the assessment. This is often a six to fifteen month effort. The vCISO oversees; the client's IT team or an MSP executes. Billed as monthly retainer plus project fees for major build-outs (enclave architecture, FIPS-validated encryption, multi-factor authentication rollouts).

- **Pre-assessment readiness.** Tabletop exercise in the format the C3PAO will run. Evidence-package preparation. Final SSP revision. Four to eight weeks. $15,000 to $35,000 fixed fee.
- **Post-certification continuous monitoring.** Quarterly evidence refresh, control attestation, incident response readiness, annual self-assessment for FCI components, three-year recertification preparation. Monthly retainer of $5,000 to $15,000 depending on scope.

Contractor profile	Typical retainer (post-cert)	Cert prep project
Small Tier-3 supplier (FCI only / Level 1)	$2,500 – $4,500 / month	$15,000 – $35,000
Mid-size CUI handler (Level 2, single site)	$5,000 – $9,000 / month	$45,000 – $120,000
Larger CUI handler (Level 2, multi-site)	$8,000 – $15,000 / month	$120,000 – $350,000
Critical-program supplier (Level 3 candidate)	$10,000 – $20,000 / month	$200,000 – $600,000

Credentials worth earning for this vertical

The CyberAB (Cyber Accreditation Body) credentials a CMMC Registered Practitioner (RP) and the more advanced CMMC Certified Professional (CCP) and CMMC Certified Assessor (CCA). The RP credential is the entry-level marker — modest barrier, modest signal. The CCP requires passing an exam with substantial body of knowledge. The CCA qualifies you to work on C3PAO assessment teams, which is a separate revenue stream from vCISO advisory but pairs well with it.

Where to find clients

National Defense Industrial Association (NDIA) chapters. Procurement Technical Assistance Centers (PTACs, now APEX Accelerators) in every state. The SAM.gov registered contractor database is searchable by NAICS code and contract history. Local defense innovation hubs (AFWERX, DIU events). Insurance brokers specializing in defense contractor policies. Existing IT MSPs serving defense contractors — many do not want to take CMMC responsibility themselves.

> **ON CMMC AND HUDSON INFOSEC**
>
> Hudson Infosec's platform is built with CMMC 2.0 alignment as a first-class design constraint. Continuous vulnerability scanning, tamper-proof event logging (Sentinel's immutable ledger maps directly to AU-9 / AU-11 evidence requirements), penetration testing on the cadence assessors expect — all available under your firm's branding. Part IV addresses how this changes the unit economics of running a CMMC-focused practice.

PART II — CHAPTER 9

Financial services & credit unions

The financial services vertical is large and fragmented. The most accessible sub-segments for a new vCISO are community banks, credit unions, registered investment advisers, and the broader set of non-bank entities that handle financial data and fall under the FTC Safeguards Rule.

Regulatory landscape

Federally insured credit unions are regulated by the National Credit Union Administration (NCUA), which has been progressively tightening cybersecurity expectations through guidance letters, the Information Security Examination program, and the cyber incident notification rule requiring 72-hour reporting of reportable cyber incidents. The NCUA Automated Cybersecurity Evaluation Toolbox (ACET) and the FFIEC Cybersecurity Assessment Tool, while not mandatory, define the de facto examination baseline.

Community banks are examined by the FDIC, OCC, or Federal Reserve depending on charter. They share the FFIEC framework and similar incident reporting rules. Registered investment advisers fall under SEC oversight; the Marketing Rule and Regulation S-P (privacy of consumer financial information) drive most cybersecurity expectations. The FTC Safeguards Rule, as amended in 2021 and effective from 2023, captures non-bank financial institutions including auto dealers, mortgage brokers, payday lenders, tax preparers above a customer count threshold, and a broad set of fintech-adjacent companies that did not historically think of themselves as financial services.

Engagement structure

Credit unions and community banks typically pursue annual third-party security assessments and follow up with monthly retainers covering vendor management oversight, incident response readiness, board reporting, and examination prep. The NCUA examination cycle (every 12 to 18 months depending on asset size and prior findings) creates a natural rhythm for engagement renewal and project planning.

Sub-segment	Typical retainer	Annual project budget
Small credit union (<$100M assets)	$3,000 – $5,500 / month	$20,000 – $60,000
Mid-size credit union ($100M-$1B)	$5,500 – $10,000 / month	$45,000 – $150,000
Community bank	$5,000 – $11,000 / month	$50,000 – $180,000
RIA / wealth advisor	$2,500 – $6,000 / month	$15,000 – $50,000
FTC Safeguards-covered non-bank	$2,000 – $5,000 / month	$10,000 – $40,000

Where to find clients

State credit union leagues, the Credit Union National Association (CUNA), Independent Community Bankers of America (ICBA) state affiliates, and state banking associations are productive. Core processor vendors and ancillary fintech vendors that sell into the same buyers will often introduce specialists when their customers ask. Investment adviser compliance consultants frequently refer cybersecurity engagements that fall outside their own remit.

PART II — CHAPTER 10

Education (K-12 and higher ed)

Education is a smaller engagement-size vertical than the others, but it has volume and high referral density. K-12 districts and small private colleges typically lack security expertise entirely and are increasingly subject to state-level requirements.

Regulatory landscape

FERPA protects student education records — narrower scope than HIPAA but structurally similar. COPPA regulates collection of data on children under 13. State laws are increasingly active: New York's Education Law §2-d for K-12, California SOPIPA, Illinois SOPPA, and similar measures in roughly half of states impose specific requirements on vendors and districts. Higher education institutions also handle research data subject to NIST SP 800-171 (for federally funded research touching CUI), HIPAA (for academic medical centers and student health), and PCI DSS (for tuition payment systems).

Engagement structure

K-12 districts often buy through a regional educational service agency or cooperative purchasing organization, which dramatically simplifies the sales motion. A vCISO contract awarded at the BOCES or regional level (in New York) or an Educational Service Center (in other states) becomes available to dozens of districts in the region. Engagement sizes per district are modest ($1,500 to $4,000 monthly), but ten districts under a single cooperative contract is a meaningful book of business.

Small private colleges and universities engage individually. Engagement size ranges from $3,000 to $10,000 monthly retainer with project work on top — Title IV financial aid information protection, research compliance, and audits driven by the federal student aid program create predictable project pipelines.

PART III — CHAPTER 11

Your service catalog

A clearly defined service catalog is the single most underrated marketing asset a new vCISO has. Clients do not know what to buy from you until you tell them. Six standard offerings, named and priced, will close more engagements than any amount of bespoke proposal writing.

The six offerings every new vCISO should publish

1. Initial Risk Assessment. A defined-scope, fixed-fee assessment delivered in four to eight weeks. Output: a current-state report mapped to the framework relevant to the client's industry, a prioritized remediation roadmap, and an executive summary suitable for board presentation. Pricing depends on framework and company size; typical range $8,000 to $40,000.

2. Security Program Development. Building the documented program from scratch — policies, procedures, the incident response plan, the disaster recovery plan, the business continuity plan, the vendor management procedure, the acceptable use policy, the data classification scheme. Eight to sixteen weeks; $20,000 to $80,000.

3. Ongoing vCISO Retainer. The recurring engagement that covers monthly oversight, quarterly business reviews, board reporting, response to client security questionnaires, and as-needed advisory. Monthly retainer of $2,000 to $15,000 depending on client size and vertical.

4. Penetration Testing. Annual or semi-annual technical testing of the client environment. External (perimeter-facing), internal (post-compromise simulation), web and API application testing, and — in industrial environments — OT/SCADA testing. Pricing depends on scope; typical range $12,000 to $80,000 per engagement.

5. Tabletop Exercise. A facilitated scenario walkthrough exercising the client's incident response plan. Two to four hours of executive engagement, preceded by scenario design and followed by an after-action report. $6,000 to $18,000 per exercise.

6. Compliance Attestation Preparation. Framework-specific preparation for a certification or audit — SOC 2, ISO 27001, HIPAA OCR readiness, CMMC Level 2, PCI DSS. Eight to twenty weeks; pricing $25,000 to $200,000 depending on framework and starting posture.

> **ON NAMING AND PACKAGING**
>
> Name your offerings concretely. "Healthcare HIPAA Risk Analysis — Initial Engagement" closes more deals than "Cybersecurity Assessment Services." The buyer should be able to read the name of the package and recognize the problem it solves. If the name is generic, the buyer will assume you are generic. (Refer back to Chapter 4.)

What not to put in the catalog (yet)

Two services tempt new vCISOs and should be deferred until the practice is stable.

Incident response retainers, in which you commit to responding to a client incident within a defined SLA, require either insurance-backed incident response infrastructure or a partnership with a digital forensics and incident response firm. Selling an IR retainer you cannot fulfill is a malpractice exposure. Defer until you have a documented partnership.

Twenty-four-by-seven security monitoring or managed detection and response is operationally expensive and competes with deeply-resourced MSSPs. A vCISO can sell evidence — continuous scanning, tamper-proof log retention, documented review cadence — without selling 24/7 alerting. Most clients do not need the alerting; they need the evidence. Sell the evidence.

PART III — CHAPTER 12

Pricing your engagements

New vCISOs systematically underprice. The reasons are predictable — underearning bias from corporate salary calibration, imposter syndrome, the urge to win the first deal at any price. The cost of underpricing in year one is high because the rate you set with your first three clients anchors the rate you can ask of all referrals from them. Underpricing early compresses your earning curve for years.

The mental model: time, complexity, and risk

Your effective hourly rate should reflect three multipliers above what an internal employee of equivalent seniority would earn:

- **Overhead.** You pay your own employer taxes, your own benefits, your own insurance, your own software, your own continuing education. A reasonable overhead multiplier is 1.4 to 1.6 above a salaried equivalent. A senior IT director making $180,000 fully loaded translates to a $250,000 to $290,000 break-even revenue requirement.
- **Utilization.** You cannot bill 40 hours a week. Sales, administration, continuing education, marketing, and unbilled goodwill consume roughly 30% of your time in a stable practice and more in year one. Realistic billable hours are 1,200 to 1,400 per year, not 2,000.
- **Risk and judgment.** You are paid for judgment, not for hours. The premium above pure-time-multiplied cost is what compensates you for the consequences of being wrong. Twenty to fifty percent above the overhead-and-utilization adjusted rate is normal for advisory work.

Putting these together: a $180,000-salaried senior IT director who wants to replicate their previous income should price advisory hours at $220 to $320 per hour, or sell retainers in the $4,000 to $10,000 monthly range depending on commitment. Pricing meaningfully below this range means you are subsidizing your client. Pricing meaningfully above it, without specialized credentials or a marquee track record, will close fewer deals than you need.

Three pricing structures, and when to use each

Monthly retainer. Default for ongoing vCISO engagements. Sets a scope of hours and types of work; bills automatically; produces predictable revenue. Use for clients you expect to serve for more than six months.

Fixed-fee project. Default for defined-scope deliverables: risk assessments, security program development, tabletop exercises, CMMC prep. The client wants budget certainty. You want margin protection. Estimate your effort honestly, add 25% buffer, present a single number.

Time-and-materials with cap. Use sparingly — for poorly scoped advisory work, vendor selection projects, or work where the client cannot yet describe what they need. Always cap with a not-to-exceed clause. Avoid pure T&M without a cap; it produces invoicing fights that destroy trust.

PART III — CHAPTER 13

Credentials worth chasing

Certifications matter in this market — not because they prove competence (they do not, much) but because they are the shorthand buyers and insurance underwriters use to filter consultants. Three or four matter enough to pursue actively; the rest are noise.

The base layer: CISSP

The Certified Information Systems Security Professional is the closest thing the field has to a journeyman credential. Required experience: five years in two of eight domains (waivable by one year with a related bachelor's degree). The exam is broad rather than deep. Holding the CISSP is table stakes for most enterprise procurement processes. Pursue this within your first six to twelve months if you do not already hold it.

Manager track: CISM and CRISC

ISACA's Certified Information Security Manager (CISM) is the management-focused counterpart to CISSP — useful if your career has been more leadership than hands-on engineering. Certified in Risk and Information Systems Control (CRISC) is the risk-management focused credential, particularly useful when you are positioning to financial services or insurance-driven buyers. Either one, not both, alongside a CISSP, is sufficient.

Vertical-specific credentials

- **Healthcare:** HCISPP (Healthcare Information Security and Privacy Practitioner) from (ISC)². A modest but useful marker.
- **Defense / CMMC:** CyberAB Registered Practitioner (RP) at minimum; CMMC Certified Professional (CCP) is the meaningful credential. CCP candidates must already hold a foundational cyber credential.
- **Financial services:** No single credential dominates, but CRISC is the most relevant of the major options.
- **Cloud:** One of AWS Certified Security – Specialty, Microsoft Certified Cybersecurity Architect Expert, or GCP Professional Cloud Security Engineer if a substantial portion of your work touches the respective platform.

Credentials not to chase

Vendor-specific certifications (firewall vendor X, SIEM vendor Y) signal operator rather than advisor. They are not negative, but they do not move the dial for advisory engagement decisions. Spend the study time on framework knowledge instead.

The CEH (Certified Ethical Hacker) is widely held but widely discounted by sophisticated buyers. If you want to credential penetration testing capability, OSCP (Offensive Security Certified Professional) carries more weight — though as a vCISO you typically partner for penetration testing rather than delivering it

personally, so the credential is more marketing than necessity.

PART IV — CHAPTER 14

The infrastructure problem

Most new vCISOs hit the same wall in month four or five. The first two clients went well. The third is signed and onboarding. The advisory work is intellectually rewarding and the rates are good. And the practice is starting to drown.

The drowning is not from the advisory work. It is from the operational infrastructure that the advisory work depends on. To deliver continuous evidence of cybersecurity oversight — which is what clients are buying, and what insurers and regulators are demanding — every client engagement requires:

- Continuous vulnerability scanning of the client's network, with regular reports the client can show to auditors, insurers, and customers.
- Periodic penetration testing, with deliverables that can be cited in compliance documentation.
- Centralized, tamper-resistant logging of security-relevant events — the evidence layer that makes "we monitor this" defensible in an audit or an incident.
- Reporting that ties the technical output back to the framework the client is being measured against, in language an executive can read.

New vCISOs typically address this by stitching together vendor portals: Tenable or Qualys for scanning, Splunk or a budget SIEM for logging, Cobalt or HackerOne or freelance pentesters for testing, and Vanta or Drata for compliance dashboarding. Each tool has its own per-seat or per-asset pricing. Each vendor wants a separate contract. Each one reports to the client in its own format. The vCISO becomes a system integrator — and not a paid one. Every hour spent assembling vendor reports into a coherent client deliverable is an hour billed at advisory rates but spent on operations work.

The math does not survive at scale. Five clients are manageable; ten are not. The vCISO either caps the practice (limiting earnings) or hires a junior operator (compressing margin and adding management overhead). The third option — and the one this guide recommends — is to outsource the infrastructure entirely to a white-label platform that delivers the operational layer under your firm's brand, and to charge the client for it as part of the engagement.

> **THE ECONOMIC ARGUMENT**
>
> A vCISO who white-labels infrastructure earns roughly the same gross revenue per client as one who assembles vendor tools — but spends 60-70% less time on operations per client. The freed time goes to advisory work at advisory rates, or to adding more clients. Either way, the practice scales beyond what an individual operator can reach on a stitched-together stack.

PART IV — CHAPTER 15

The Hudson Infosec vCISO Program

Hudson Infosec runs a white-label partner program for vCISO firms. The program exists for exactly the reason described in Chapter 14: vCISOs need an operational layer beneath their advisory work, and they should not have to build it themselves.

What the program is

The program is infrastructure-as-a-service for vCISO consultancies. The partner brings the client relationship and the strategic advisory work. Hudson Infosec provides the scanning, penetration testing, tamper-resistant event logging, AI-driven report analysis, and the white-label delivery layer that puts everything in front of the client under the partner's own brand.

Element	What it is
Membership fee	$0 / month. No recurring fee for partner status.
Scanner nodes	Physical hardware shipped to client sites, plus virtual VM and ISO formats. Partner rate $175 / node / month, minimum 5 per order.
Other services	30% partner discount on penetration testing, retainers, virtual nodes, ISO subscriptions, and API testing — applied automatically at invoice.
Contract term	Month-to-month, no minimum commitment, cancel any time.
White-label scope	Partner's firm name, logo, contact info, and report footer applied to PDFs and customer-facing emails.
End-client capacity	Unlimited. One partner can serve any number of end clients.
Onboarding	Apply at hudsoninfosec.com/vciso-apply; admin-vetted; typically active same business day.

What the partner delivers under their own brand

- **Continuous network vulnerability scanning** via Ayewo scanner nodes — physical hardware, virtual VMs, ISO images, AWS-ready cross-account AMIs, and OT-edition variants for industrial environments. Weekly automated scans, AI-analyzed PDF reports delivered under the partner's brand.
- **AI-powered penetration testing** across External Blackbox, Internal Grey Box, API testing (OWASP API Top 10), SCADA and ICS engagements, and combined and recurring retainer packages. White-label deliverables with AI-generated executive narratives and remediation prioritization.

- **Immutable security event logging** via the Sentinel platform — a tamper-proof ledger backed by cryptographic chaining, with fast search through OpenSearch and role-based access. The retention layer for cyber-insurance evidence, SOC 2, ISO 27001, HIPAA, and CMMC.
- **End-client management** built into the partner portal — add, edit, and archive clients; each one gets their own scanner deployments, locations, and report archive.
- **Built-in white-label branding** — logo, firm name, footer, and contact information applied automatically to every PDF report and client-facing email. Hudson Infosec is removed from the customer-visible surface (Ayewo and Sentinel product names remain, since they are the platform brands).

Unit economics

The realistic monthly numbers for a vCISO practice with ten end-clients on the Hudson Infosec stack:

End-client size	What you pay HSEC	What you can charge	Your gross margin
Small (1–2 nodes + monthly scans + Sentinel)	$350 – $700	$2,000 – $3,500	$1,500 – $2,800
Mid-size (4–8 nodes + qtrly pentest retainer + Sentinel)	$1,000 – $2,000	$5,000 – $10,000	$4,000 – $8,000
Enterprise (8+ nodes + ongoing pentest + multi-site)	$2,500 – $5,000	$12,000 – $25,000	$9,500 – $20,000

A ten-client portfolio mixing all three sizes generates $15,000 to $80,000 monthly gross margin from the Hudson Infosec layer alone — before any of the strategic advisory revenue that sits on top. No upfront capital expenditure. No inventory. No vendor management overhead beyond the single Hudson Infosec relationship.

HOW PARTNERS GET STARTED

1. Apply at hudsoninfosec.com/vciso-apply — firm name, your name and email, the white-label name your clients will see, expected client count, and a short note about your practice.
2. We review applications individually, typically within one business day.
3. You receive a welcome email with a portal sign-in link.
4. In the portal, configure white-label branding, add your first end client, and place your first node order.
5. Scans run on the next schedule; deliverables ship under your brand. First clients can be live within a week.

PART IV — CHAPTER 16

Mapping the platform to each vertical

The same platform serves different verticals in different ways. The table below maps the Hudson Infosec stack to the engagement patterns described in Part II.

Vertical	Primary platform use	What you deliver under your brand
Healthcare	Continuous Ayewo scanning of clinical networks; Sentinel ledger for HIPAA §164.312(b) audit-control evidence; OWASP API testing for patient portals and EHR integrations.	Quarterly Risk Analysis updates, monthly evidence packets for OCR posture, white-labeled penetration test reports for BAA partner reviews.
Legal	Ayewo virtual nodes inside firm networks; Sentinel retention of authentication and access logs; external penetration testing aligned to outside-counsel security questionnaires.	Annual security posture report for client questionnaire responses, tabletop exercise outputs, ABA Model Rule 1.6 reasonable-efforts documentation.
Manufacturing	Ayewo OT Edition scanner nodes on segmented industrial networks; passive Modbus / DNP3 / IEC-104 discovery; SCADA-specific penetration engagements.	Supplier security attestation packets for OEM customers, NIST SP 800-171 self-assessment evidence, OT inventory and risk reports for plant leadership.
Defense (CMMC)	Ayewo continuous scanning of CUI enclaves; Sentinel immutable logging mapping to AU-9 / AU-11 / SI-4 controls; recurring penetration testing in the cadence C3PAOs expect.	System Security Plan supporting evidence, POA&M milestone tracking, pre-assessment readiness packages, post-certification monthly attestations.
Financial services	Ayewo network scanning across branches and remote workforce; Sentinel as the audit log of record for examination support; API and web application testing on member-facing portals.	Quarterly board cyber reports, NCUA / FFIEC examination preparation packages, FTC Safeguards Rule evidence binders.
Education	Ayewo scanning across district or campus networks; Sentinel logging for FERPA access-monitoring evidence; periodic application testing of SIS and LMS systems.	State education-law compliance packets (NY §2-d, IL SOPPA, CA SOPIPA), annual security attestation for vendor onboarding, board-level cyber risk reports.

The key observation: the platform output is the same engine in every vertical, but the deliverable that lands on the client's desk is framed for the regulatory framework they care about. That framing is your

advisory work — the platform produces the evidence; you produce the narrative.

Where the platform runs: U.S. models on our own hardware

The entire Hudson Infosec platform — the scanning back end, the Sentinel event ledger, report generation, and every AI-driven step from analyzing scan results to drafting executive narratives and prioritizing remediation — runs on hardware Hudson Infosec owns and operates. The AI uses only U.S.-developed models. Client scan data, findings, and event logs are not hosted with a public cloud provider, and they are never sent to a public AI service or an outside model provider.

The AWS-ready Ayewo node described in Chapter 15 is a deployment option for clients who want a scanner inside their own AWS account. It is not where the platform runs.

Regulated buyers ask about this more every quarter. Security questionnaires, outside-counsel guidelines, and insurance applications now routinely ask whether a vendor uses AI, which models, and where client data is processed. For a partner, the answer is short and defensible in every vertical:

- **Defense (CMMC).** Data about CUI enclaves stays on hardware the platform provider owns, with no hand-off to a cloud host or commercial AI provider — one less external party to account for in the System Security Plan.
- **Healthcare.** Findings on systems that hold ePHI are not shared with a cloud host or outside AI vendor, so there is no additional subprocessor to add to the client's Business Associate inventory.
- **Legal.** Confidential details of a firm's network stay out of public AI tools — the point outside-counsel guidelines and ABA Model Rule 1.6(c) reasonable-efforts reviews increasingly ask firms to document.
- **Financial services and education.** One vendor running its own models keeps third-party AI risk out of the vendor-management file under GLBA, FFIEC guidance, and state student-privacy laws.

> **WHAT TO TELL CLIENTS**
>
> “Our platform runs entirely on hardware our provider owns and operates, and its AI uses only U.S.-developed models. Your data is never hosted in a public cloud or sent to an outside AI service.”
>
> Partners can use this wording as written in questionnaire responses, proposals, and sales conversations.

PART V — CHAPTER 17

Your first 90 days

This chapter is operational. The goal: have one paying client and a credible pipeline by day 90.

Days 1 – 14: foundation

- Form the LLC. Register for an EIN. Open the business bank account and a separate credit card.
- Bind professional liability and cyber liability insurance — $1M / $1M minimum. Carrier appetites vary; brokers like Founder Shield and Embroker specialize in technology consulting placement.
- Pick your vertical. Write a one-paragraph description of who you serve and what you sell. Read it aloud. If you cannot say it in three sentences, narrow it further.
- Reserve the domain name and stand up a one-page website with a clear description of services and a contact form. Do not invest in elaborate site design at this stage; clarity beats polish.
- Set up a LinkedIn presence positioning you as a vCISO in your chosen vertical. Connect with every former colleague, vendor, and customer who might refer business. Tell them what you are now doing.

Days 15 – 45: market entry

- Apply to the Hudson Infosec vCISO Partner Program (or equivalent infrastructure partner). Configure white-label branding. You will want this in place before your first sales conversation, because prospects will ask how you deliver.
- Develop the six standard service offerings described in Chapter 11, named for your vertical. Set published prices.
- Build a standard engagement letter. Have a consulting-experienced attorney review it. Total cost should be under $2,000 for a one-time review.
- Identify ten target prospects in your vertical within a defined geographic or industry reach. Find a warm path to each — a former colleague, a shared trade association, a referral source. Send ten introduction emails. The first three responses will tell you whether your pitch is tuned correctly.
- Speak somewhere. A regional bar association cybersecurity committee, a manufacturing extension partnership lunch, a state credit union league webinar — find one venue and offer a 30-minute presentation. This is faster lead generation than any cold outreach.

Days 46 – 90: first client and pipeline

- Close your first engagement. The pricing will feel low; the relief will be substantial. Sign it. Deliver well.
- Use the first engagement as the proof point in conversations with the second and third prospects. "I just completed a HIPAA Risk Analysis for an outpatient surgical practice in [region]" is the most useful sentence in your sales repertoire.
- Establish weekly delivery rhythm using the platform infrastructure: scans running, reports generated, evidence accumulating. The infrastructure does the operational work; you do the advisory work.

- By day 90, target three signed engagements and at least five active conversations in the pipeline. This is achievable in most regional markets if specialization is genuine and pricing is at market rates.

WHAT SUCCESS LOOKS LIKE AT 90 DAYS

Three signed engagements at market rates is roughly $9,000 to $30,000 monthly recurring, depending on vertical and engagement size. This is enough to cover your fully-loaded overhead and most of a modest salary. It is not enough to be the goal. The goal is the pipeline: by the end of day 90, you should have a credible path to 8-10 clients within twelve months. That is when the practice becomes an asset rather than a job.

PART V — CHAPTER 18

Pitfalls, and how to avoid them

New vCISOs make six predictable mistakes. None of them are fatal. All of them slow the practice by six to twelve months when they happen.

Pitfall 1: scope creep without scope conversation

The first client will ask for things outside the engagement letter. The instinct is to do them as a goodwill gesture. The cost is months of operating below the margin you priced. The discipline: a short, friendly scope conversation each time a request falls outside scope. "That falls outside the current engagement, but I can put together a short proposal to add it — would you like me to?" Almost all clients respect the professionalism. The few who do not are not clients you want.

Pitfall 2: taking the wrong vertical at the wrong price

A second client appears outside your chosen vertical, offering a fee below your published rate. The temptation is severe in month four. The cost is twelve to eighteen months of compounding distraction. Polite decline; refer if possible to a colleague in that vertical; preserve the relationship for the future.

Pitfall 3: doing the work yourself

Senior IT operators have a natural impulse to dive in and fix the broken configuration personally. As a vCISO this is the most dangerous habit. Every hour spent doing operator work is an hour priced at operator rates and an hour the client does not learn from. Write the recommendation. Hand it over. Follow up.

Pitfall 4: undocumented advisory

Verbal advice is forgettable, undefendable, and unmarketable. Every meaningful advisory conversation produces a one-paragraph memo logged into the engagement record. When the client's auditor asks what oversight is in place, the memos are the evidence. When the client's board asks what they have been getting for their retainer, the memos are the answer. When the client refers you to a peer, the memos are the shareable artifact that explains your value.

Pitfall 5: under-investing in administrative infrastructure

Bookkeeping, contract management, time tracking, expense tracking — the boring administrative apparatus that small consulting firms either set up early or suffer through later. Set it up early. QuickBooks Online or Xero plus a contractor accountant ($150 to $300 monthly) saves more time in year two than it costs in year one.

Pitfall 6: skipping insurance until "after the first client"

Professional liability and cyber liability coverage should be in place before the first engagement letter is signed. The premium for the first year is modest; the exposure of operating uninsured is not. This is one of the few absolute rules in this guide.

PART V — CHAPTER 19

Next steps

This guide has covered a lot of ground. To summarize what to actually do next, in order:

Decide the vertical

Spend a week. Read the chapter in Part II that matches your background most closely. Talk to two or three former colleagues or contacts in that vertical. Confirm there is at least one specific buyer profile within geographic reach. Commit.

Set up the business

Form the LLC. Bind insurance. Stand up the website. Write the engagement letter. The whole sequence should take four to six weeks of evening and weekend work, less if you can dedicate weekdays.

Establish the infrastructure

Apply to the Hudson Infosec vCISO Partner Program. Configure your white-label branding. Provision a sample environment so that when you demonstrate the platform on a sales call, you can show actual scans, reports, and dashboards under your firm's name rather than describing them in the abstract.

> **APPLY TO THE PROGRAM**
>
> Apply at **hudsoninfosec.com/vciso-apply**. Onboarding is typically same business day. The application asks for firm name, your contact information, the white-label name your clients will see, expected client count, and a short note about your practice. There is no membership fee and no minimum commitment.

Start selling

Identify ten target prospects. Send the first ten outreach emails. Book the first speaking engagement. Have the first ten conversations. The first signed engagement letter usually arrives between week six and week twelve of active outreach, in our experience watching new partners ramp.

Stay in touch

If this guide is useful, the most valuable next step is a conversation. We talk with prospective partners every week — about whether the program fits, what your practice could look like in twelve months, and what specific obstacles might apply to your vertical and geography.

CONTACT

Email info@hudsoninfosec.com

Apply hudsoninfosec.com/vciso-apply

Hudson Infosec, LLC · Poughkeepsie, NY · UEI F8WESK541XW1 · CAGE 9YD00 · NYS MWBE certified

Good luck building the practice. The market needs it.

HUDSON INFOSEC

Cybersecurity for regulated industries

Build the cybersecurity practice your career has been preparing you for.

The vCISO market is hungry for seasoned IT leaders who can translate technical risk into business decisions. Hudson Infosec provides the operational stack — scanning, pentest, immutable logging, AI-driven analysis — under your brand, so you can focus on the advisory work that only you can do.

Free to join. Pay only for what your clients use.

Apply at hudsoninfosec.com/vciso-apply

Questions: info@hudsoninfosec.com

Hudson Infosec, LLC · Poughkeepsie, New York

CMMC 2.0 aligned · NYS MWBE certified · UEI F8WESK541XW1 · CAGE 9YD00