

Virtual CISO vs In-House CISO: Operating Model Decision Matrix



IG-Smart Ltd · Practical Guide Collection · 25 October 2026

General information and original working aids; not legal advice, certification, clinical authorisation or regulatory approval.
NHS identity appearing in retained illustrative artwork does not imply NHS approval or endorsement.

Use this guide to make a better-evidenced decision. This is general information and an original working aid, not a client-specific legal opinion, certification, clinical safety authorisation or regulatory approval. Apply the relevant jurisdiction, current requirements and competent professional review to your circumstances. Examples are illustrative unless expressly attributed.

Your first three steps

1. Define authority, incident coverage and the execution capacity the business requires.
2. Compare like-for-like scope and first-year versus recurring costs.
3. Use the operating-model gates to choose an accountable, sustainable arrangement.

How to choose accountable cyber leadership, governance capacity and a defensible engagement model without confusing advisory services with management responsibility or independent audit

Cost-claim safeguard: Neither a percentage saving nor a standard retainer represents a reliable market benchmark without like-for-like scope, total employment and provider costs, required coverage, buyer-side support, specialist testing, availability and assumptions. Use the comparison method below; do not present a universal 60–70% saving as a verified IG-Smart outcome.

Executive proposition: A vCISO is not automatically a cheaper substitute for a full-time executive. The right model depends on risk complexity, management accountability, authority, delivery capacity, coverage, board reporting and continuity. An outsourcing contract can supply expert capacity; it cannot transfer directors' governance responsibilities by default.

For: CEOs, Boards, CROs, CIOs, General Counsel, procurement leads, PE portfolio operators and security leaders planning a vacant or evolving leadership role. **Scope:** strategic procurement and governance decision support; not a salary survey, labour market forecast or commitment that IG-Smart accepts every executive or operational appointment described.

Executive briefing — six questions before choosing a model

1. Which cyber risks, services, subsidiaries and regulatory frameworks must the leadership role cover?
2. Does the organisation need an accountable employed executive, retained independent adviser, fractional leadership, or a hybrid team?
3. Who controls budgets, accepts risks, signs decisions and responds to incidents outside office hours?
4. Is there enough internal implementation capacity to act on specialist advice?
5. What coverage, succession and conflicts arrangements will protect continuity?
6. How will effectiveness be measured beyond meetings held or documents written?

The UK Cyber Governance Code of Practice addresses directors' own responsibilities in five areas: risk management, strategy, people, incident planning/response/recovery and assurance/oversight. Choosing a virtual CISO does not remove these board-level responsibilities. [S1][S2]

1. Four operating models and when they fit

Model	Typical use	Strength	Main limitation
In-house CISO	High complexity, sustained demand, major people/platform leadership	Dedicated embedded authority and immediate context	Recruitment, succession and single-person concentration
Retained vCISO	Need for senior cyber governance, board reporting and defined specialist capacity	Flexible senior oversight, structured reporting and access to specialist expertise	Authority/availability depend on contract and internal owners
Hybrid model	In-house security/IT management plus retained strategic cyber adviser	Combines context, execution and external challenge	Ambiguity unless responsibilities are explicit
Interim executive	Defined vacancy, transition or transformation	Time-bounded capacity to stabilise leadership	Transition planning and actual executive authority must be defined

A project security consultant or penetration tester does **not** automatically deliver the mandate of a virtual CISO. Scope matters more than job title.

2. The IG-Smart Cyber Leadership Fit Test – eight decision gates

Gate	Question	Evidence	No-go or escalation
L1 Exposure	What is the consequence of cyber failure?	Important services, systems, data and regulated duties	Unknown consequential scope
L2 Authority	Who owns cyber decisions and delegated risk acceptance?	Board and executive RACI	Adviser's authority assumed without delegation
L3 Cadence	How much sustained strategic work is required?	Workload, programme and meeting calendar	Under-resourced retained scope
L4 Execution	Can internal teams implement control improvements?	Owners, skills and backlog	No delivery capacity
L5 Incident	Who leads at 03:00 during a significant incident?	Escalation rota, contracts, tabletop evidence	Gap between expectations and coverage
L6 Independence	Can independent audit be obtained without self-review?	Segregation and conflict review	vCISO asked to audit own implementation
L7 Continuity	Can the mandate survive absence, transition and provider exit?	Named contacts, knowledge transfer and succession	Single point of failure
L8 Economics	Does the model generate adequate control and business value?	Fully loaded cost scenarios and outcomes	False low-cost comparison

The Fit Test is an original screening methodology; it is not a regulatory certification or numerical guarantee of outcomes. Failing a critical authority or incident-coverage gate cannot be offset by a low retainer.

3. The hidden cost of the 'cheap vCISO' comparison

A defensible financial comparison uses **total comparable capability**, not salary versus monthly retainer alone. For an employee, include recruitment, employer costs, specialist deputies, training, tooling, holiday cover and the organisation's actual incident support arrangements. For a vCISO, include the contracted mandate, capacity and availability, technical implementation resources, additional expertise, incident retainers, travel, reporting, onboarding and change requests.

Do not assume that a retained adviser provides unlimited availability, 24/7 SOC monitoring, penetration testing, breach response or accredited certification. If a service is excluded, cost its necessary complement rather than claiming the risk has disappeared.

Buyer-side economic model

First-year cash cost = recurring leadership fees or employment costs + required supporting delivery capacity + incident/recovery provision + separate assurance costs + one-off recruitment, mobilisation and transition.

Steady-state annual cost = the same recurring components, excluding one-off costs unless they genuinely recur. Avoid double-counting items already included in a fee or employment-cost estimate. Model ordinary demand and a stressed demand scenario separately.

Unpriced exposure is a separate decision input. Record uncovered dependencies, capacity constraints and consequences alongside the cost comparison. Do not add an arbitrary financial value to an unknown risk merely to make a cheaper model appear equivalent. Estimates require stated assumptions; the guide supplies no market salary, guaranteed saving or risk-price benchmark.

4. Which responsibilities can the role actually perform?

Responsibility	Board/executive retained	Possible vCISO activity	Internal delivery dependency
Risk appetite and acceptance	Decision authority remains with appointed management	Interpret exposure and recommend options	CRO and service owner
Cyber strategy	Approve business priorities and investment	Develop roadmap and reporting	Programme manager/IT
Policy and controls	Allocate owners and resources	Design standards and challenge control maturity	Control owners
Third-party assurance	Decide procurement and risk acceptance	Risk-based supplier review and escalation	Procurement and contracts
Incident command	Approve responsibilities and delegated decisions	Advisory leadership if contracted	On-call incident manager and recovery teams
Board reporting	Directors challenge and decide	Evidence-led reporting and options	Reliable management evidence
Independent audit	Protect audit objectivity	Coordinate preparation; separate assurance if permitted and independent	Internal audit/qualified separate provider
Privacy/clinical interfaces	Appropriate legal and clinical owners decide	Coordinate with specialists	DPO/CSO/General Counsel

5. Seven engagement clauses that matter more than the job title

1. **Mandate:** precise services, sectors, legal entities and outcomes.
2. **Authority:** approvals the adviser can recommend versus decisions reserved for management.
3. **Capacity:** retained time, locations, meeting schedule, response assumptions and surge terms.
4. **Incident boundary:** when the adviser is available; what constitutes an emergency and what is out of scope.
5. **Evidence and reporting:** access to records, management cooperation and board-report cadence.
6. **Independence:** conflicts, self-review limits and separate audit procurement.
7. **Continuity and exit:** replacement personnel, secure handover, ownership of deliverables and transition.

An engagement described as “virtual executive” may still be advisory in law and practice. Do not promise delegated statutory board authority, 24/7 incident response or outcomes without an express contractual basis.

6. Leadership model comparison for different organisations

Early enterprise SaaS selling into regulated procurement: a retained vCISO may help establish governance, ISO readiness and supplier questionnaires while the internal technical team builds controls. Independence boundaries must be preserved for Clause 9.2 audit.

Complex financial services organisation: dedicated leadership may be important for regulatory interfaces, operational resilience, outsourcing concentration and constant risk decisions; a hybrid team can add challenge and specialist expertise. Check specific FCA/PRA requirements rather than assuming one mandated role for all firms.

NHS technology vendor: the role may coordinate DSPT, cyber governance and assurance evidence, but it cannot replace the necessary clinical safety or information governance professional roles.

Large group with newly acquired subsidiaries: interim/hybrid leadership may help harmonise reporting and accountability, but jurisdictional, privacy and transfer obligations require specific review.

7. A weighted model-selection matrix without false precision

A buyer may score candidate models against **governance fit (20), risk complexity (15), senior availability (15), operational execution (15), incident capability (15), independence (10) and continuity/transition (10)**, totalling 100 illustrative points. Rate each from 0 to 4 based on documented evidence. **Mandatory gates on authority, incidents, competence and conflicts remain independent of the arithmetic.** Weightings are a proposed tool, not proven prediction of outcomes.

For each model record the source of the score. “Vendor says 24/7” is not proof of a staffed incident function; verify contractual and operational evidence.

8. A realistic 90-day mobilisation outline — illustrative, not an entitlement

Discovery and mandate: confirm critical services, risk ownership, board expectations and constraints. **Baseline:** map highest-consequence exposure, evidence limitations, existing control programmes and unfinished commitments. **Action plan:** agree achievable work packages with resources and decision

ownership. **Board evidence:** produce the first decision-grade pack, document accepted uncertainties and establish incident escalation. **Operational handover:** integrate control owners, calendars, suppliers, exercises and succession arrangements.

The order and duration of these activities depend on actual engagement scope. This outline must never be interpreted as a guaranteed 90-day implementation or included services at an entry price.

9. Eighteen procurement questions

- Which senior practitioner will actually deliver the work?
- What relevant expertise and independence claims are verified?
- Which legal entities, services and regulated obligations are in scope?
- Who can accept material risk, approve spend and stop deployment?
- What evidence will reach the board and in what form?
- How many retained days and meetings are included?
- How are urgent issues handled outside business hours?
- Is incident-response engineering included or separately contracted?
- Which internal staff must execute the recommendations?
- Who maintains supplier oversight and third-party assurance?
- Does readiness support create an internal-audit self-review issue?
- How does the provider handle sickness, resignation or key-person loss?
- What are the boundaries of penetration testing or security operations?
- Can the provider support multiple jurisdictions without overstating legal coverage?
- Who owns work papers, risk registers and reports on exit?
- What is the handover process to a future in-house CISO?
- How are confidentiality, access and conflicts addressed?
- What are the base and surge costs under realistic demand?

10. Board decision briefing

Risk context: __; **models compared:** __; **critical requirements:** __; **mandatory gate outcomes:** __; **comparative weighted findings:** __; **capacity gap:** __; **incident escalation owner:** __; **cost scenarios and assumptions:** __; **proposed operating model:** __; **authorised approver:** __; **transition and review trigger:** __.

The board should decide based on defensible governance and ability to execute—not solely the provider's proposed day rate or a branded role title.

11. Buyer FAQs

Does a vCISO remove the board's responsibility? No. It can support oversight and expert advice; accountability remains with authorised directors and management.

Can a vCISO deliver an internal audit? Only if the actual assignment meets applicable objectivity and impartiality requirements; prior implementation work may create conflicts.

Does a vCISO replace a DPO or CSO? No. These are distinct specialist/legal/professional roles requiring separate suitability and scoping.

Is there a regulatory requirement for every business to employ a CISO? No universal rule; check applicable sector and organisational arrangements.

Can a vCISO operate 24/7? Only under a defined, resourced contract; do not infer it from the title.

What should procurement compare? Mandate, authority, competence, availability, execution capacity, assurance independence, continuity and fully loaded economics.

12. Commissioning the right support

Next step: Talk to a Senior Practitioner about cyber leadership accountability, risk complexity, retained capacity and reporting needs.

Sources

- [S1] UK Government, Cyber Governance Code of Practice <https://www.gov.uk/government/publications/cyber-governance-code-of-practice/cyber-governance-code-of-practice>
- [S2] NCSC, Cyber Security Toolkit for Boards <https://www.ncsc.gov.uk/collection/board-toolkit>
- [S3] NCSC, Principle C: People <https://www.ncsc.gov.uk/collection/board-toolkit/principle-c-people>