InfoSecAI

A BRIEF FOR BOARDS & EXECUTIVES

PLAYBOOK · 2026

# The vCISO 90-Day Plan

The structured first three months. The artefacts the board will see. The questions the regulator will ask. Distilled from twenty years of senior security leadership across financial services, telecommunications, energy, healthcare and the public sector.

AUTHORED BY

**Paul Jolliffe**

Founder & Director, InfoSecAI · Senior CISO / vCISO · CISSP · ISO 27001 Lead Auditor · MBA

01 · WHY THE FIRST 90 DAYS MATTER

# The first 90 days set the next 900.

When a fractional or interim CISO joins, the first 90 days establish the trust, evidence and operating rhythm the rest of the engagement will run on. Get them right and the function compounds. Get them wrong and you spend months unwinding mis-prioritised work, opaque risk decisions, and a board that no longer reads the security pack.

This document sets out the plan I run on every engagement. It is not a generic 30-60-90. It is the working method I have built across senior security roles at IBM, KPMG, PwC, T-Systems (Deutsche Telekom, where I led a £12m cyber transformation), Philip Morris International, Britannia Financial Group, MTN and Phoenix Software, plus current advisory engagements at InfoSecAI.

It is structured into three phases — **Discover, Decide, Direct** — each producing a defined artefact set. Each phase has a clear purpose and a clear handover into the next.

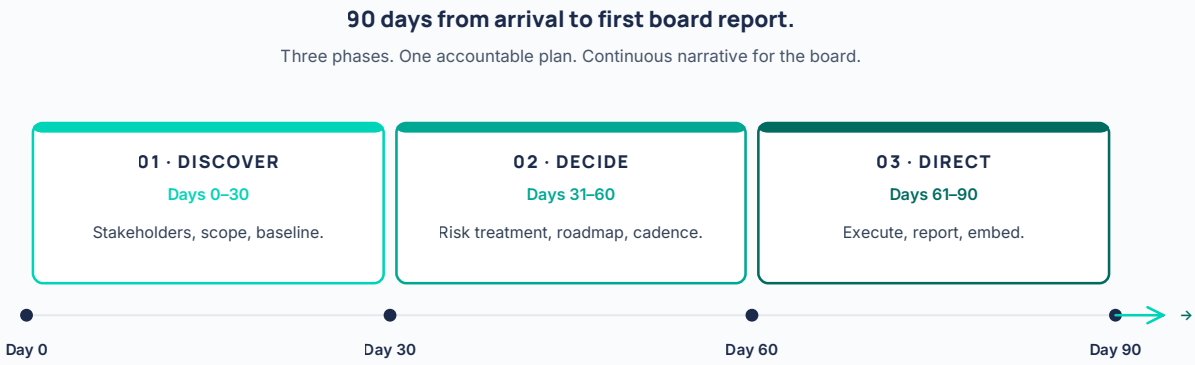
| 3 | 12 | 1 |
|---|---|---|
| phases of 30 days | milestones tracked weekly | board pack delivered by Week 12 |

> **Reading note.** If you are a CFO, CEO or board member commissioning a vCISO, the milestones to push for are listed at the end of each phase. If you are a security leader stepping into the role yourself, the practitioner detail is in the workstream narratives.

02 · THE THREE PHASES

# Discover. Decide. Direct.

Three phases of 30 days. Each ends with a defined artefact set the board, executive team or regulator can rely on. The cadence is non-negotiable; the content adapts to the organisation.




The 90-day arc — from arrival to first board pack to operating rhythm.

PHASE 01 · DISCOVER

### Days 0–30

Build the truthful picture. Stakeholders, scope, assets, obligations, risks, current control posture, immediate quick wins.

PHASE 02 · DECIDE

### Days 31–60

Make the decisions that shape the next 12 months. Risk appetite, target operating model, roadmap, governance cadence, KPIs.

PHASE 03 · DIRECT

### Days 61–90

Move from deciding to executing. Operating rhythm in motion. First board pack delivered. Steady-state cadence in place.

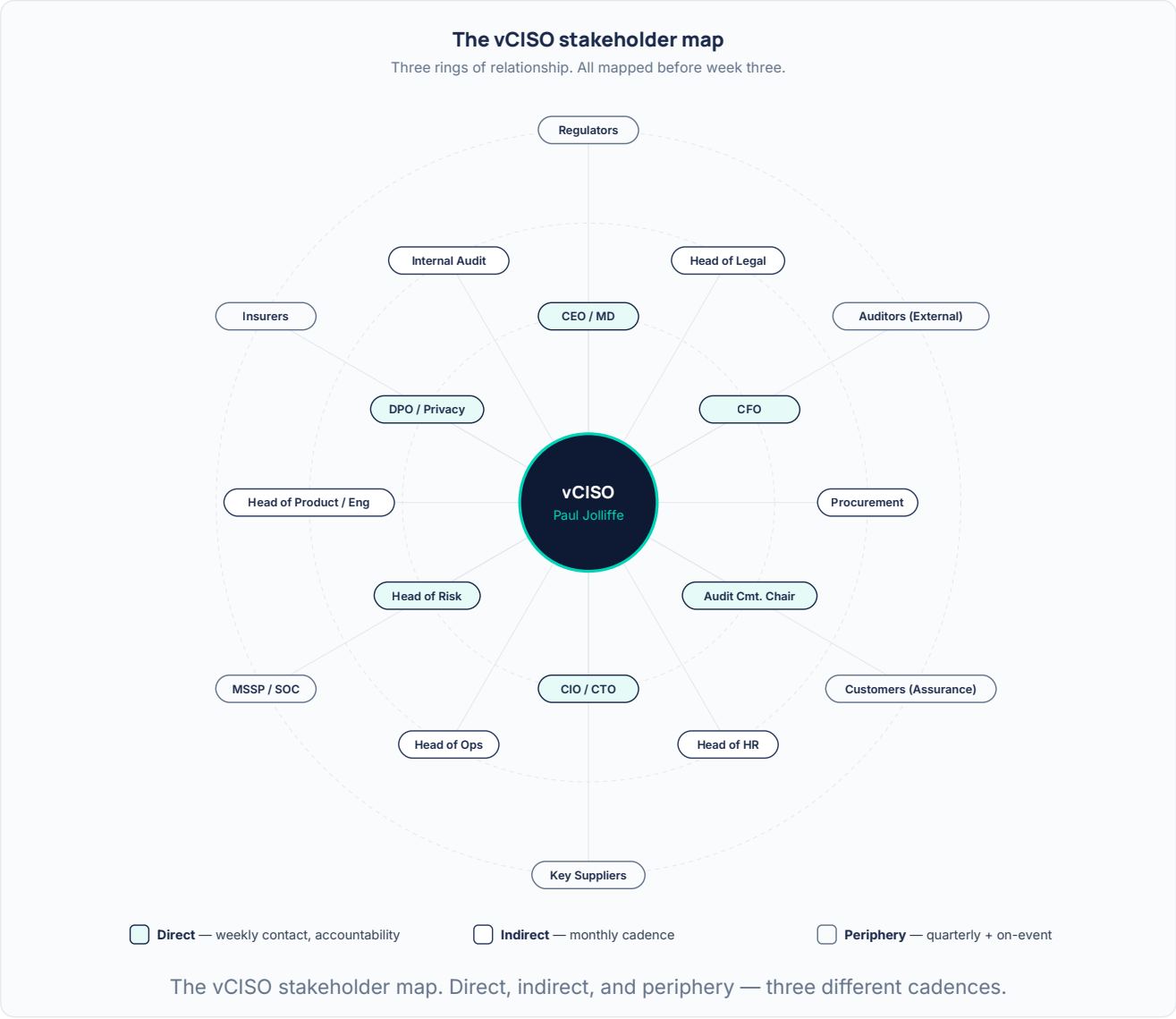
PHASE 01 · DAYS 0–30

# Discover.

The first thirty days are about **signal collection**. Most security mistakes are made early because the leader acted on assumed context rather than verified context. Your job in Phase 01 is to build a picture you can defend.

## Workstream 1.1 — Stakeholder mapping.

Within the first three weeks, every stakeholder in the diagram below should have been met, briefed, and asked the same three questions: what is the risk that worries you most; what do you think is working; what would you like the security function to stop doing. Their answers are gold. They tell you the political topology of the organisation, where the budget will come from, and what the board will not tolerate.




The vCISO stakeholder map. Direct, indirect, and periphery — three different cadences.

### Workstream 1.2 — Asset and obligation inventory.

You cannot protect what you cannot see, and you cannot prove compliance against an inventory that does not exist. Within 21 days, the function should have a working hardware/software inventory, a Records of Processing (RoPA) inventory, an AI tool inventory, a data classification register, and a regulatory obligation register. The first three are usually partially complete already; the last two are typically missing or stale.

### Workstream 1.3 — Maturity baseline.

By end of Week 4, you produce a **baseline maturity assessment** against the dominant framework for your sector — typically ISO 27001:2022 for general industry, NIST CSF 2.0 for North America-aligned organisations, DORA for financial services, or DSPT and CAF for UK public sector. The output is not a heat-map for its own sake; it is the document that anchors the risk-treatment decisions you will make in Phase 02.

### Workstream 1.4 — Quick-win identification.

Identify three to five Wave-0 actions that can be delivered in the first 60 days at low cost and high credibility return. They are not the most strategic work; they are the work that demonstrates motion. Typical Wave-0 candidates: enabling MFA on a remaining estate, killing a known-stale privileged-access pattern, formalising an IR runbook, or introducing a phishing simulation cadence.

**Phase 01 deliverables (signed off by Day 30)**

- Stakeholder map with documented appetites and concerns.
- Asset, obligation, RoPA and AI inventories — current within ±10%.
- Maturity baseline against dominant framework.
- Risk register v1 (issues, not yet treatments).
- Wave-0 action list with owners and dates.

> **What good looks like.** By Day 30 a CFO should be able to ask "what do you actually own?" and you can hand over a single page that summarises every above-the-line answer. If you cannot, you have not finished Discover.

PHASE 02 · DAYS 31–60

# Decide.

Decide is where most fractional CISO engagements stall. The temptation is to accelerate into delivery before the decisions that frame delivery have been made and signed off. Discipline through Phase 02 is what turns the next nine months into a programme rather than a backlog.

## Workstream 2.1 — Risk-based prioritisation.

Take the maturity baseline and the risk register from Phase 01 and convert them into a treatment plan. Each risk gets one of four treatments — accept, transfer, avoid, mitigate — with an owner, a deadline, and a residual-risk projection. Risks that are accepted are signed by the appropriate executive; that signature is the most important document in the security function.

## Workstream 2.2 — Target operating model.

Draft a two-page Security Target Operating Model: structure, capabilities, build vs. buy decisions, MSSP boundary, in-house specialism, escalation chain. The TOM does not need to be perfect; it needs to be specific enough to make the next twelve months of resourcing decisions defensible.

## Workstream 2.3 — Governance cadence.

The cadence is what scales the function. Below is the four-tier rhythm I implement. Each tier has a fixed agenda, a defined artefact, and a documented escalation path to the tier above. After Phase 02 it should run without your active management.


The four-tier governance rhythm. Each tier feeds the one above it.

### Workstream 2.4 — Roadmap (Wave plan).

The roadmap is grouped into waves of work, not sprints of activity. Wave 0 (already done) is the credibility delivery. Wave 1 closes the highest-residual-risk items. Wave 2 closes audit and certification gaps. Wave 3 builds the operating model. Wave 4 begins horizon investment (AI governance, post-quantum readiness, operational resilience). The roadmap is a one-page artefact with named owners and budget envelopes; it is the document the board approves, not the underlying ticket list.

### Workstream 2.5 — KPI and KRI set.

Pick a small number of KPIs and KRIs you can sustain. The temptation is to design twenty; the reality is that you can keep ten current and the board will read four. Mine are typically: MFA coverage, vulnerability SLA compliance, MTTD/MTTR, IR exercise pass rate, supplier-risk re-attestation timeliness, training compliance, residual-risk movement, audit-finding ageing, regulatory-action exposure, and cyber-insurance posture.

**Phase 02 deliverables (signed off by Day 60)**

- Risk treatment plan with executive sign-off on every accepted risk.
- Two-page Security Target Operating Model.
- Four-tier governance cadence operational, with terms of reference for each forum.
- Wave-based roadmap with named owners and quarterly budget envelopes.
- KPI / KRI set with baseline values and reporting cadence.

> **What good looks like.** By Day 60 the Audit Committee Chair should be able to read the security narrative without your presence. If they still need you in the room to interpret the artefacts, you have not finished Decide.

PHASE 03 · DAYS 61–90

# Direct.

Direct is where the artefacts produced in Phases 01 and 02 stop being plans and start being operating reality. Phase 03 is light on new artefacts and heavy on cadence, kickoffs and embedment. By Day 90 the function should run without your daily intervention.

## Workstream 3.1 — Operating rhythm in motion.

Each of the four governance tiers should hold its first instance under the new cadence by Day 75. The first occurrence is run by you with the relevant chair. The second occurrence is chaired by the chair, with you in advisory mode. By the third, the rhythm runs without prompting.

## Workstream 3.2 — Wave-1 delivery.

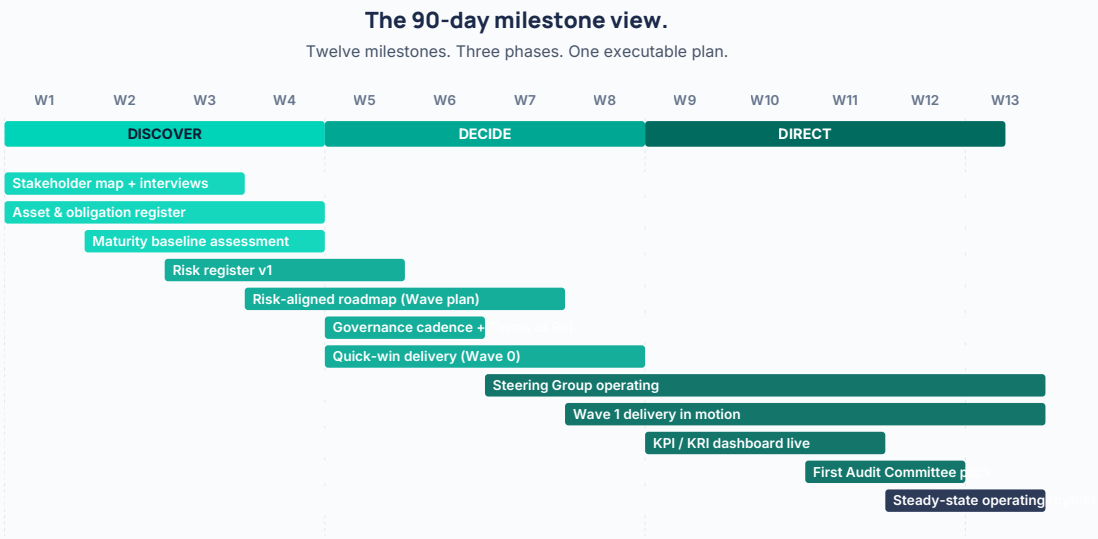
Wave 1 starts in earnest in Week 9. The vCISO does not own the delivery; the relevant accountable executive does. Your role is to maintain the narrative, escalate blockers, and keep the executive accountable for the deadline they signed up to in Phase 02. This is the difference between a CISO who runs everything and a CISO who runs the system.

## Workstream 3.3 — First board pack.

By Week 11–12 you produce the first formal Audit Committee or Board pack. Twelve pages maximum. Cover sheet plus one page on each of: regulatory horizon, risk appetite trends, KPI movement, audit-finding ageing, top-three current issues, top-three forward decisions, financial outlook, regulatory-engagement summary, third-party risk top items, and a one-page request for the board (typically an investment decision or a risk acceptance).

## Workstream 3.4 — Embedment and steady state.

By Day 90 the function transitions out of "stand-up" mode into "operate" mode. The vCISO's hours pattern usually shifts from 4 days a week to 2–3 days a week, with the structure now sustaining itself through the operating rhythm and the named executives owning their workstreams.




The 90-day milestone view — twelve milestones plotted across the three phases.

## Phase 03 deliverables (signed off by Day 90)

- All four governance tiers running unprompted.
- Wave-1 delivery underway with named executive accountability.
- First Audit Committee / Board pack delivered.
- KPI / KRI dashboard live with at least one full reporting cycle.
- Steady-state operating rhythm signed off by the accountable executive.

04 · COMMON PITFALLS — AND HOW TO AVOID THEM

# The five mistakes I have made so you don't have to.

| PITFALL | WHAT IT LOOKS LIKE | HOW TO AVOID IT |
|---|---|---|
| **Discover slips into design** | By Week 3 you are sketching architectures rather than mapping stakeholders. Inevitable temptation; almost always wrong. | Defer all architectural work to Phase 02. Phase 01 is signal collection only. |
| **Roadmap by activity, not outcome** | Roadmap reads as a list of projects rather than a narrative of risk reduction. Boards lose interest by Page 2. | Tie every wave to a residual-risk movement target. Lead with outcome, follow with activity. |
| **Risk acceptance without signature** | Several risks "accepted" verbally; nothing on file. Falls apart in audit. | Every accepted risk has a named executive signature, dated, with review trigger conditions. |
| **Board pack is a status report** | Pack reads like a project update. Board cannot tell what to do. | Board pack is decision-driven. Each page ends in a question or a decision request. |
| **Cadence collapses without you** | The forums stop running when you reduce hours. Function reverts. | Chair the second instance, not the first. Embed ownership early. Be replaceable by Day 90. |

05 · ABOUT INFOSECAI

# If this is the operating discipline you want for your security function.

InfoSecAI provides fractional CISO, vCISO and senior security advisory services to UK organisations. We help boards, executives and security leaders deliver practical governance, controls and operating-model change across information security, GRC and AI governance.

**20+**
years senior CISO / vCISO experience

**£12m**
largest cyber programme delivered

**7**
sectors regularly served

## Engagement models

- **Fractional CISO** — 1–3 days per week on retainer, for organisations between £10m and £300m revenue.
- **Interim CISO** — 4–5 days per week for 3–9 months, bridging a permanent appointment or an uplift programme.
- **Advisory retainer** — board-level advisory by call and quarterly review, for existing CISOs needing senior peer challenge.
- **Programme delivery** — discrete programmes (ISO 27001, DORA readiness, AI governance) priced by scope and outcome.

## Sector experience

Financial services (FCA-regulated), telecommunications, energy, healthcare, technology, public sector, professional services. Past engagements: IBM, KPMG, PwC, T-Systems, Philip Morris International, Britannia Financial Group, MTN, Phoenix Software, Lloyds Banking Group, Petrofac, Bestway Wholesale, Vodafone.

### To talk about your first 90 days

A 30-minute conversation about your current security and AI governance position, the outcomes the board wants to see, and whether a fractional or interim CISO model is the right fit. No charge, no obligation.

Email **paul.jolliffe@infosecai.net** or book directly: **infosecai.net**.

Founder credentials: MBA (Henley Business School) · CISSP · ISO 27001:2022 LA / LI / IA · PRINCE2 Practitioner.