RETACH

vCISO ENGAGEMENT FRAMEWORK

Fixed-Scope Virtual CISO Engagement — Governance, Roles & Operating Model

Document Control	
Status	Version 1.0
Applies to	RETACH Digital Ltd — Virtual CISO (vCISO) Fixed-Scope Engagement
Classification	Template — completed and signed for each client
Governing law	Republic of Kenya
Related documents	Mutual NDA · Scope of Services / SOW Template

1. Purpose & Scope of this Framework

This Framework sets out how RETACH Digital Ltd ("RETACH") delivers the Virtual Chief Information Security Officer (vCISO) service under the Fixed-Scope Engagement model, and the umbrella terms under which individual vCISO engagements — and future retainer tiers, once launched — operate.

It defines roles and functions, the onboarding sequence, governance cadence, independence safeguards, escalation path, exit terms, and the commercial and legal terms for the relationship. Every element is mapped to the S.I.N.S. Framework, ISO/IEC 27005 and the NIST Cybersecurity Framework 2.0 (Govern function) (Section 12), so a client board can see the engagement rests on recognised standards, not only on RETACH's own methodology.

This document is the umbrella Framework. Each individual engagement (e.g. a specific audit, ISO 27001 readiness project, policy build, or board roadmap) is separately scoped, priced and timed under its own Scope of Services / Statement of Work (SOW), executed under this Framework.

2. vCISO vs Managed Security — Boundary of Responsibility

RETACH's vCISO service is a strategy, governance and accountability layer. It is deliberately kept distinct from Managed Security, the operational layer that executes day-to-day controls (whether delivered by RETACH's Managed Security service, the client's own IT team, or an OEM/partner). The vCISO directs and holds the client accountable to a risk-based plan; Managed Security executes it.

vCISO (Governance Layer)	Managed Security (Operational Layer)
Sets security strategy, policy and risk appetite with the Board	Implements and operates security controls (firewalls, EDR, patching, backups)
Owns the risk register and its board-level reporting	Executes remediation tasks assigned from the risk register
Oversees vendor/OEM selection and governance (vendor-neutral)	Operates the selected vendor tools day to day
Chairs incident response governance and post-incident review	Executes incident response actions (containment, recovery)
Tracks regulatory alignment (e.g. Data Protection Act 2019)	Implements technical controls that support compliance
Commissions the Risk Delta re-run to prove risk reduction	Provides the evidence RETACH scores the Risk Delta against

RETACH may deliver Managed Security itself under a separate SOW, or the client may use its own team/another provider — the vCISO's governance role and vendor-neutral posture do not change either way.

3. Engagement Model

RETACH runs vCISO engagements on a two-layer paper trail:

- Master Engagement Framework (this document) + Mutual NDA — signed once, covers the relationship.
- Scope of Services / SOW — signed per engagement, sets the fixed scope, deliverables, price and duration for that specific piece of work.

Current Fixed-Scope menu (launch offer): Security Audit (Digital Resilience Assessment); ISO/IEC 27001 Readiness; Security Policy Build; Board Security Roadmap; Post-Incident Review. Retainer tiers (Advisory, Program, Executive) are available on request as the practice grows, and would run under a Retainer SOW referencing this same Framework — no new NDA required.

4. Roles & Functions (RACI)

R = Responsible, A = Accountable, C = Consulted, I = Informed.

Activity	Board / Exec Sponsor	Client IT Lead	RETACH vCISO	RETACH Delivery	Ops / MSSP
Set risk appetite & strategic priorities	A	C	R	I	I
Approve security policy	A	C	R	C	I
Own & maintain risk register	I	C	A/R	C	I
Prepare board risk reporting	I	C	A/R	C	-
Day-to-day control operation	I	A	C	R	R
Incident response coordination	I	C	A	R	R
Vendor / OEM governance	I	C	A/R	C	I
Post-remediation Risk Delta re-run	I	I	A	R	C

5. Onboarding — 30/60/90-Day Plan

Days 1–30: Foundation

- NDA and Framework executed; kickoff workshop with Board/Exec Sponsor and Client IT Lead.
- Document review: existing policies, prior audit findings, asset/identity inventory.
- Draft risk register opened; RACI (Section 4) confirmed with named individuals.
- Access and evidence requests issued for the applicable Fixed-Scope engagement.

Days 31–60: Baseline

- Baseline assessment executed against the specific SOW (audit / ISO 27001 gap / policy gap / post-incident findings).
- S.I.N.S. pillar scoring captured where the engagement type produces it.
- Draft policy, roadmap or findings artifacts circulated for client comment.
- First board-ready summary presented.

Days 61–90: Governance Live

- Final SOW deliverable(s) signed off.
- Standing governance cadence (Section 6) begins.
- Escalation path (Section 8) walked through and tested with named contacts.
- 30/60/90 review: confirm success criteria met, agree next engagement or renewal.

6. Cadence & Board Reporting

- Monthly — RETACH vCISO and Client IT Lead: operational check-in, risk register movement.
- Quarterly — RETACH vCISO and Board/Executive Sponsor: strategic review, S.I.N.S. pillar scorecard, Risk Delta status.
- Ad hoc — triggered by a material incident, a regulatory inquiry, or a risk register item crossing an agreed severity threshold.

Standard board report contents: S.I.N.S. pillar scorecard, Risk Delta (baseline vs. current), top open risks with owners and target dates, and regulatory/Data Protection Act 2019 status.

7. Independence & Conflict of Interest

- RETACH's vCISO recommendations are vendor-neutral by default.
- Where RETACH also resells OEM products (e.g. ESET, Sophos, JumpCloud, Segura, Lansweeper) under a disclosed reseller relationship, any recommendation involving those products is flagged as such, alongside at least one alternative.
- No RETACH staff member holds an undisclosed financial interest in any vendor recommended to a client.
- Any circumstance that could compromise the independence of a recommendation is disclosed to the client before the recommendation is made.

8. Escalation Path

Severity	First Responder	Escalates To	Target Response
Routine query	RETACH vCISO	—	2 business days
Operational issue	Client IT Lead + RETACH vCISO	RETACH Delivery Lead	1 business day
Material risk / incident	RETACH vCISO	RETACH Directors + Board/Exec Sponsor	Same business day
Dispute on scope or deliverable	Both parties' Exec Sponsors	Mediation (Section 11)	Per Framework terms

9. Exit & Handover

- On termination or non-renewal, RETACH hands over the full risk register, all board reports, policy documents and Risk Delta history, in client-owned formats — no proprietary tooling lock-in.
- A handover call is held within 10 business days of notice being given by either party.
- Fees for work performed up to the effective date are settled per the applicable SOW; no further fees accrue after that date.

10. Intellectual Property

- The client owns deliverables specific to its environment: its policies, its reports, and the content of its risk register.
- RETACH retains ownership of its underlying methodology — the S.I.N.S. Framework, the CRQ Engine, and its templates and pre-existing IP. The client receives a licence to use deliverables produced from them for its own internal purposes.

11. Commercial & Legal Terms

Term & Renewal

This Framework runs for 12 months from the date of signature and renews automatically for successive 12-month terms, unless either party gives at least 30 days' written notice before a renewal date. Where a specific SOW states its own term or duration, that SOW's term governs for that engagement.

Fees

Fees are set per the applicable SOW or Quotation. RETACH Digital Ltd is not currently VAT-registered; invoices are issued accordingly.

Liability

RETACH's aggregate liability under this Framework and any SOW issued under it is capped at the total fees paid by the client under the specific SOW giving rise to the claim. This cap does not apply to breach of confidentiality, gross negligence, wilful misconduct, or infringement of intellectual property rights.

Confidentiality

Confidentiality obligations are set out in the separate Mutual NDA, which is incorporated into this Framework by reference and signed alongside it.

Termination for Cause

Either party may terminate immediately on a material breach that remains uncured 14 days after written notice, or on the other party's insolvency.

Governing Law & Dispute Resolution

This Framework is governed by the laws of the Republic of Kenya. Any dispute is first addressed by good-faith negotiation between the parties' Executive Sponsors (14 days), then by mediation (a single mediator, costs shared equally). If unresolved, either party may refer the dispute to the courts of Kenya, seated in Nairobi.

12. Framework Alignment

How the elements of this Framework map onto S.I.N.S., ISO/IEC 27005:2022 and the NIST Cybersecurity Framework 2.0 (Govern function).

Framework Element	S.I.N.S.	ISO/IEC 27005:2022	NIST CSF 2.0
Governance & oversight (Sections 1–2)	Security	Risk context & communication	GOVERN (GV.OC)
RACI & risk register ownership (Sections 4, 9)	All four pillars	Risk identification & evaluation	GOVERN / IDENTIFY (GV.RM, ID.RM)
Policy build (Section 5)	Systems / Security	Risk treatment	GOVERN (GV.PO)
Board cadence & reporting (Section 6)	Security	Communication & consultation	GOVERN (GV.OV)
Incident escalation (Section 8)	Security / Network	Risk monitoring & review	RESPOND / RECOVER
Vendor / OEM governance (Section 7)	Infrastructure / Network	External party risk context	GOVERN (GV.SC)

13. Sign-off

By signing below, both parties agree to operate under this Framework, subject to the Mutual NDA and any SOW executed under it.

Client	RETACH Digital Ltd
Name: _____	Name: _____
Title: _____	Title: _____
Signature: _____	Signature: _____
Date: _____	Date: _____