SORAMI / SECURITY

vCISO retainer: scope one-pager

For teams where nobody owns security and a customer, a board or an auditor is now asking who is accountable.

What the retainer covers

- A named senior contact, not a rotating queue.
- A fixed number of days each month, agreed up front.
- A written monthly report you can forward unedited.
- A prioritised roadmap with owners and dates.
- A risk register maintained monthly, not annually.
- Attendance at board, customer review and auditor calls.
- Customer and insurer questionnaires reviewed before you answer.
- Incident response plan written and exercised once a year.

What it is not

- Not a full-time CISO. The hours are bounded and written down.
- Not a compliance rubber stamp. We will not sign off untested controls.
- Not a penetration tester. Testing is scoped separately.
- Not round-the-clock incident response. We help you plan and exercise.
- Not your auditor. We prepare you for the body that attests.
- Not hands-on remediation. Engineering is a separate scope.

Days and term

We do not publish a default number of days or a default minimum term. A team with one cloud account and a regulated team with an auditor need different cadences. Both are agreed on the scoping call and written into the scope before anything starts.

Cadence

- A standing monthly working session with engineering.
- A written report before each board or leadership cycle.
- Ad hoc attendance at customer and auditor calls in scope.
- One incident response exercise each year.

The first 90 days

Phase	What happens	What you receive
Weeks 1 to 2	Asset, identity and vendor picture. Interviews with engineering and support.	A current-state summary and the initial risk register.
Weeks 3 to 6	Gaps ranked by exposure and by who is asking. Quick wins started.	A prioritised roadmap with an owner and a date per item.
Weeks 7 to 12	Roadmap execution oversight. Policy set aligned to how you work.	The first two monthly reports and an exercised response plan.

How the retainer ends

- Either side may end the retainer in writing after the agreed term.

- The risk register, roadmap and policy set are yours and stay with you.
- We write a handover note naming what is open and who owns it.
- If you hire a full-time lead, we brief them and step back.

What we are not

Sorami is not ISO 27001 certified, not SOC 2 audited, and not a CREST member company. We are not an ASD-endorsed or IRAP provider. We prepare your organisation for the body that certifies, audits or attests.

Sorami Consulting Pty Ltd, ACN 702 116 452, Australia. hello@sorami.com.au. Scope, fee and term are confirmed in writing before work begins.