

SAMPLE

Fractional CISO Engagement Kit

The opening of CISO-Engagement-Proposal.docx, one of 9 files in the kit.

<https://solasai.net/products/fractional-ciso-kit/>

Fractional CISO Engagement Proposal

Template with a worked example for an AI startup client

Product: Fractional CISO Engagement Kit, version 3.0, 19 October 2026. **Classification:** Purchaser use only, customize before use. Solas AI, solasai.net.

How to use this document

Part A is the proposal template with bracketed placeholders. Part B is the same proposal filled in for a fictional client, Example Labs, a 40-person AI startup selling to enterprises, so you can see what a complete one reads like. Keep the structure; replace every bracket; delete Part B before sending.

Part A. Template

1. The situation

[Client] is a [stage] company of [headcount] people building [product] for [customers]. Enterprise prospects have begun sending security questionnaires and asking for SOC 2; the engineering team owns security by default and has no dedicated owner for it; and the board has asked for a view of cyber risk. The company needs a security program and a person accountable for it, without a full-time executive hire at this stage.

2. What a fractional CISO does here

A named security executive, part time, who owns the security program: sets the roadmap, makes the risk decisions, presents to the board, runs vendor and customer security conversations, and directs the engineers who implement controls. Not a penetration tester, not an MSP, not a compliance clerk. The engagement is measured by the deliverables in Section 4 and the risk reduction reported monthly.

3. Scope by phase

Phase	Months	Work	Deliverables
Assessment and foundation	1 to 2	Asset and data inventory; risk assessment; gap analysis against [SOC 2 / ISO 27001 / NIST CSF]; policy set; incident response plan; identity and endpoint baseline	Risk register, gap report, 12-month roadmap, policy set v1, IR plan v1
Implementation	3 to 6	Controls build-out with engineering: SSO and MFA everywhere, logging and alerting, vulnerability management, vendor review process, secure development practices, AI-specific controls (model vendor terms, prompt injection testing, data handling)	Monthly reports; control evidence; vendor register; first tabletop exercise
Audit readiness and maturation	7 to 12	Evidence collection; auditor selection and readiness assessment; customer security questionnaire library; trust page; metrics and board reporting cadence	Readiness report; questionnaire library; quarterly board briefings; year-two roadmap

4. Ongoing deliverables

Monthly: the Monthly Security Posture Report (template in this kit), a working session with engineering leadership, and the risk register update. Quarterly: the Board Security Briefing (template in this kit), the maturity assessment score, and a roadmap review. Always: security questions from customers and prospects answered within [two business days]; incident command when an incident occurs; vendor security reviews within [five business days] of request.

5. What is not included

Hands-on implementation beyond configuration guidance (engineering does the work, or a separate engagement scopes it); penetration testing and audits (procured from third parties, which the CISO selects and manages); 24x7 monitoring (an MDR provider, which the CISO selects); legal advice; writing production code.

The sample ends here. The full document runs about 1,203 words; the kit holds 9 files. Version 2.2, 19 October 2026. Buy it at <https://solasai.net/products/fractional-ciso-kit/>, 14-day refund for any reason.