Kailash Consult Free resource · kailashconsult.com/resources

New Security Lead 30-Day Plan

The 10 things to have ready before your security lead starts, a week-by-week first month, and the questionnaire answers they will need first.

How to use

- Founders and CTOs: finish the 'Before day 1' section before the hire starts, so month one is spent closing gaps, not finding them.
- Security lead: use weeks 1-4 as your plan. Each task has a 'done when' so progress is visible to leadership.
- The last section lists the questionnaire answers buyers ask for first. Draft them with the Enterprise Security Review Kit.

Example answers and mappings are templates, not facts about your company. Edit every bracket and validate each statement before sharing it with a customer or auditor.

Before day 1 (founder / CTO)

ID	Task	Why it matters	Done when
B01	List every open customer security ask: questionnaires, report requests, deadlines, deal size.	Tells the new lead what revenue is waiting on security.	One list with owner and due date for each ask.
B02	Collect every past questionnaire and answer in one folder.	Most new questionnaires repeat old questions.	Folder shared with the security lead.
B03	Build a system inventory: apps, cloud accounts, data stores and their owners.	You cannot secure what you cannot see.	Inventory sheet with an owner per system.
B04	Draw a simple data map: what customer data you hold, where it lives, who can access it.	Almost every buyer question traces back to this.	One-page diagram, even if rough.
B05	List admin access for cloud, identity provider, source control and production.	Admin sprawl is the first thing auditors and attackers find.	Named list of admins per system.
B06	Gather existing policies and docs, even drafts.	Avoids rewriting what already exists.	Docs in one folder with last-updated dates.
B07	List your vendors, including AI and model providers.	Buyers ask for your subprocessors early.	Vendor list with what data each touches.
B08	Find the last pen test, scan or audit results.	Shows the starting point and open findings.	Reports saved with findings status.
B09	Decide the target: SOC 2 Type I or II, ISO 27001, or both, based on what customers actually ask for.	Prevents a year spent on the wrong framework.	Written decision with target month.

Kailash Consult

ID	Task	Why it matters	Done when
B10	Set budget and access: compliance tooling, auditor and pen test shortlist, accounts for the new hire.	The hire can act in week one instead of waiting.	Budget approved; accounts created.

Week 1: listen and map

ID	Task	Why it matters	Done when
B11	Meet sales and rank stalled or upcoming deals by security asks.	Puts revenue at the center of the security plan.	Ranked list agreed with sales.
B12	Walk the system inventory and data map with engineering.	Finds what the documents missed.	Inventory and data map corrected.
B13	Read the past questionnaires and mark repeat questions.	Builds the answer library fast.	Top repeat questions listed.
B14	Quick check: MFA everywhere, SSO coverage, offboarding speed.	The three gaps buyers and attackers hit first.	Gaps listed with owners.
B15	Set up a security@ inbox and a draft trust page.	One front door for customers and researchers.	Inbox live; trust page drafted.

Week 2: fix the obvious

ID	Task	Why it matters	Done when
B16	Close MFA and SSO gaps found in week 1.	Removes the most common breach path.	100% MFA on workforce and admin accounts.
B17	Remove stale accounts and excess admin rights.	Shrinks the blast radius.	Admin list reduced and signed off.
B18	Turn on audit logging and basic alerts in cloud and identity provider.	You need logs before you need them.	Logs retained; alerts routed to a channel.
B19	Enable dependency scanning, secret scanning and branch protection.	Catches the cheapest-to-fix problems.	Settings on for all production repos.
B20	Enforce the laptop baseline through MDM.	Endpoints are evidence auditors check.	Disk encryption and updates enforced.

Week 3: write it down

ID	Task	Why it matters	Done when
B21	Approve a core policy set (10-12 policies).	Policies are required evidence for SOC 2 and ISO 27001.	Policies approved by leadership.
B22	Run risk assessment version 1.	Drives priorities and is required by both frameworks.	Risk register with owners and treatments.
B23	Review your top 10 vendors.	Vendor risk is a standard buyer question.	Vendor register with review dates.

Free to use inside your company. Not for resale. kailashconsult.com/resources

ID	Task	Why it matters	Done when
B24	Finalize the incident response plan and book a tabletop.	Shows you can handle a bad day.	Plan approved; tabletop on the calendar.
B25	Build answer library version 1 from the Enterprise Security Review Kit.	Turns questionnaires from weeks into days.	Top 50 answers drafted and validated.

Week 4: prove it

ID	Task	Why it matters	Done when
B26	Select the auditor and the pen test firm.	Lead times are the usual bottleneck.	Engagements signed with dates.
B27	Produce a readiness gap list with owners and dates.	Turns the framework into a project.	Gap list reviewed with leadership.
B28	Publish the trust page with documents available on request.	Answers half the questions before they are asked.	Trust page live.
B29	Present a 90-day roadmap to leadership.	Gets budget and priority locked in.	Roadmap approved.
B30	Measure questionnaire turnaround time.	The number sales cares about.	Baseline recorded; target set.

Questionnaire answers they will need first (see Enterprise Security Review Kit)

ID	Task	Why it matters	Done when
B31	A03: SOC 2 report or ISO 27001 certificate, or a readiness date.	Usually the first gate in procurement.	Answer drafted.
B32	A12: MFA enforcement.	Asked in nearly every review.	Answer drafted.
B33	A19 and A20: encryption at rest and in transit.	Baseline technical control.	Answer drafted.
B34	A28: last penetration test.	Independent evidence buyers trust.	Answer drafted.
B35	A30: logging and monitoring.	Shows you would notice an attack.	Answer drafted.
B36	A37: subprocessor list.	Needed for their privacy review.	Answer drafted.
B37	A42: breach notification timeline.	Often written into the contract.	Answer drafted.
B38	A45: backups and restore testing.	Business continuity check.	Answer drafted.
B39	A49: is customer data used to train AI?	Now standard for any product with AI.	Answer drafted.
B40	A08: offboarding speed.	Common audit and buyer finding.	Answer drafted.

Free resource from Kailash Consult. Free to use inside your company. Not for resale or redistribution.
kailashconsult.com/resources