

Starting a Security Program

Three milestones, for companies that do not have one yet.

Most companies do not start a security program because they planned to. A customer sends a questionnaire, a regulator sends a letter, or something goes wrong. This is the map, whether you are legal, compliance, a founder, or the person who was handed it. Work the milestones in order. How long each one takes depends on your company, not a calendar. It will change on contact with your business, and that is fine.

1 MILESTONE Get the Lay of the Land

Learn how the business makes money, what it cannot afford to lose, and who is holding it together, before you buy a tool or write a policy.

WHAT YOU HAVE

- ☐ List every system, SaaS and AI tool you run on. Expect triple what people report.
- ☐ Map where your data lives, vendors included, and how it gets there.
- ☐ Name the three losses the business cannot survive, then price one hour of downtime.

WHAT YOU OWE

- ☐ List what binds you and who enforces it: GDPR, NIS2, customer security clauses.
- ☐ Read the security and data clauses in your biggest contracts. The fine print counts.
- ☐ Collect what customers already asked for: questionnaires, DPAs, audit requests.

WHO HOLDS IT TOGETHER

- ☐ Name one owner for security, with hours and a budget line, even part time.
- ☐ Ask each team what they need to get the job done, before you ask anything of them.
- ☐ Write down what would stop the business if one person left tomorrow.

2 MILESTONE Build the Foundation

Make the right thing the easy thing. Guardrails before blame, and the version each team can run.

GUARDRAILS

- ☐ MFA and one login everywhere. If one click can take you down, fix the architecture, not the user.
- ☐ Find the one thing everyone complains about in security, and remove it first.
- ☐ Make leaving a deprovisioning step: access off the same day, keys rotated.

BASICS

- ☐ Back up what matters, away from the systems it comes from, and test one restore.
- ☐ Keep devices updated and protected, with logs someone actually reads.
- ☐ Sign an incident-response partner now. Write the one-page plan: who calls whom.

PAPER

- ☐ Write policies people will read: acceptable use, access, data, incidents.
- ☐ Keep a vendor list: a DPA and a risk tier for each, and a consequence per tier.
- ☐ Set rules for AI tools: what data may go in, who owns each, what it may touch.

3 MILESTONE Validate and Gain Momentum

Share the responsibility, celebrate the people who flag things, and prove it holds when you are not in the room.

TEST IT

- ☐ Run one tabletop: ransomware, a lost laptop, or a fake CEO payment request.
- ☐ Verify payment requests on a channel you already had, never the one supplied.
- ☐ Audit your approval limits by pricing a request one dollar under each of them.

SHARE IT

- ☐ Keep a risk register with an owner and a date on every item.
- ☐ Brief leadership on the gaps, starting with the ones you already have controls around.
- ☐ Keep receipts as you go: the evidence customers, auditors, and insurers ask for.

KEEP IT RUNNING

- ☐ Put it on the calendar: quarterly access reviews, yearly policy review, training on hire.
- ☐ Give public credit to whoever flags a risk or reports a problem. Security is a shared win.
- ☐ Decide if SOC 2 or ISO 27001 is your next step, based on what customers ask for.

MILESTONE CHECK

Progress, or just busy?

At the end of each milestone, count what you can tick today, not what you plan to. **Six of nine and you are on track.** Fewer is not a failing grade, it is where your next stretch of effort goes. The plan will change. The trajectory does not have to.