

SECURITY LEADERSHIP

The first 90 days of security leadership

A practical starting sequence for a new security lead: understand the business, choose priorities and establish useful oversight.

By Haroon Mahmood

A business can reach the point where security needs leadership before it needs a full-time security executive. Customer questions take longer to answer. IT has a growing list of findings. Several people own parts of the problem, but nobody can explain which decisions matter most.

The first few months should make that situation easier to manage. You need an agreed view of the risks, people who can act on them and a realistic delivery plan. This guide sets out a practical starting sequence for a new security lead or a business appointing fractional support. The timings are a planning aid, not a promise that every organisation can complete the work in 90 days.

Begin with a mandate people understand

In a previous in-house role, I established a business's first dedicated information security function. The work included its strategy, risk register, policies, assurance approach and a security committee. Those pieces had to work together. The risk register fed decisions; the committee gave leaders a regular forum to address issues and support delivery.

Start by agreeing what the security lead is being asked to achieve. Is the immediate need to understand exposure, prepare for customer scrutiny, improve a struggling programme or help the business expand? Put the purpose in a short engagement brief with an executive sponsor, scope, access to the right people and a realistic time commitment.

Be explicit about authority. The security lead can assess and recommend; accountable business leaders need to make the decisions that sit within their authority. Agree who may approve expenditure, accept remaining risk or pause a high-risk change. Fractional support also needs clear arrangements for availability, escalation and cover. An advisory engagement does not automatically provide round-the-clock incident response.

The NCSC's [Cyber Security Toolkit for Boards](#) puts governance and oversight firmly within leadership's remit. Use it to frame the sponsor's role, then document how decisions will work in your business.

Days 1 to 30 - establish the picture

Meet the people who run the business as well as the people who run its technology. Ask what must keep working, where sensitive information moves and which commitments customers depend on. Include someone who deals with the practical work: approving access, releasing software, paying suppliers or supporting customers.

Select a small number of important services and trace their dependencies. A diagram showing the service, owner, main systems, external providers and recovery arrangements is often more useful at this stage than an incomplete inventory of everything the organisation owns.

Read existing findings before commissioning another assessment. Look at incident reviews, testing reports, audit actions, customer commitments and the current change plan. Check dates and scope. Ask what has changed since the evidence was collected and which issues have already been addressed.

Follow a few controls through in practice. For example, ask the team to show how a supplier's access was approved, how an important service was restored during a test, or how an urgent vulnerability became an assigned task. Agree sampling and permissions first. Record what the sample supports and what remains uncertain.

If you find an active incident or a serious exposed weakness, use the existing escalation route immediately. The discovery phase must not delay containment or urgent treatment.

By the end of this stage, aim to have:

- A short description of the business services and information that matter most.
- A working list of material risks, with evidence, uncertainty and accountable owners.
- A map of existing controls and the teams or suppliers operating them.
- Immediate actions already assigned, with interim protection where appropriate.
- A list of decisions the sponsor needs to make.

NIST's [Small Business Quick-Start Guide](#) offers a useful way to check coverage across governance, identification, protection, detection, response and recovery. It is a reference for the conversation; the output still needs to reflect your services and resources.

Days 31 to 60 - choose what to deliver

Bring the evidence back to the people who will do the work. Check that the description is fair and that proposed actions address the underlying issue. If a supplier can access more systems than its work requires, for example, the response may include a technical restriction and a clearer approval process between the service owner and IT.

Choose a manageable set of priorities. Explain the business consequence, the exposure, the existing protection and the reason for acting now. Identify dependencies: a new access control may depend on knowing which accounts exist; a recovery improvement may require an agreement with a supplier.

Give each priority a delivery owner and a separate risk owner where those roles differ. Record the agreed result, target date, resources, interim measures and how completion will be checked. When work cannot be funded or scheduled, make the remaining exposure and decision visible. A postponed task should not disappear from the risk discussion.

Use one existing management forum if it can make the necessary decisions. Add a separate security meeting only when it serves a clear purpose. Send a concise paper before the meeting: what changed, what is blocked and which decision is required. Maintain a decision log afterwards.

The companion guide on [turning findings into an improvement plan](#) gives a fuller method for this stage.

Days 61 to 90 - show that the arrangements work

Start checking completed work against the agreed result. If a team says privileged access has been tightened, look for evidence that the intended accounts are covered, exceptions are controlled and the process can be maintained. Where independent testing is needed, make that part of the scope rather than treating a progress report as proof.

Rehearse a business decision under pressure. A short discussion exercise could explore a supplier outage or suspected compromise of an important account. Agree the purpose and boundaries, bring the right decision makers together and record where authority or information is missing. Keep the exercise separate from live systems.

The NCSC's [Exercise in a Box](#) provides free material for this kind of rehearsal. Its [getting-started guidance](#) also covers preparation and following up the discussion. An exercise can reveal gaps in plans and decisions; it does not prove that a technical recovery will succeed.

Use what you learn to revise the next quarter's work. Identify processes that still depend on one person, actions waiting for a business decision and controls that have not yet been tested. Make the handover usable even if the security lead is unavailable.

A useful first-quarter report

Keep the report short enough for someone to read before a meeting. For each significant risk, show:

- **Business consequence:** the service, commitment or information that could be affected.
- **Current position:** evidence gathered, protection in place and important uncertainty.
- **Action and ownership:** the next deliverable, accountable people and dependencies.
- **Decision needed:** the choice, resources or acceptance required from leadership.
- **Next check:** when and how the position will be reassessed.

For illustration, a recovery item might say: "The customer portal has daily backups, but restoration of its application configuration has not been demonstrated. The platform owner will run an agreed recovery test. Leadership needs to confirm the acceptable period of disruption so the result can be

judged.” That gives the meeting something concrete to decide and the technical team something concrete to verify.

What to expect from fractional support

Before appointing support, ask who will perform the work, how findings become delivery tasks, what evidence you will retain and how the arrangement fits your internal team. Agree the distinction between advice, programme coordination and hands-on implementation. Set a review point so the commitment can change as the business develops.

Kurosec's fractional security leadership helps establish these priorities and keep decisions moving. If you need to build the underlying capabilities, security programme development can provide a defined piece of work with an agreed handover.

Contact us to discuss where leadership would make the most useful difference.