

IMPROVEMENT PLANNING

Turning security findings into a practical improvement plan

Turn a report into owned work: prioritise exposure, agree realistic actions and check that the changes address the findings.

By Haroon Mahmood

The report has arrived. It contains useful findings, several recommendations and more work than the team can take on at once. The next task is to decide what changes, who will deliver it and how you will know the problem has been addressed.

This is where security judgement meets delivery. A technically sensible recommendation can stall because it needs a decision from finance, a change by a supplier or time from the same engineer already assigned to three other priorities.

In previous in-house roles, I partnered with HR and Finance leaders to translate technical findings into business impact, treatment options and decisions about the risk that would remain. I also built security governance and worked with accountable owners to take remediation through to closure. That experience informs the approach below: make the decisions visible, and make completion demonstrable.

Deal with urgent exposure immediately

Triage the findings before scheduling a planning workshop. Evidence of an active compromise, exposed credentials or a critical weakness being exploited in an affected service needs prompt escalation through the appropriate incident or urgent change process.

Confirm the exposure, involve the people who operate the service and agree immediate protective action. Consider the operational consequences and whether specialist incident support is needed. Applying a patch alone does not establish that an already compromised system is safe.

The NCSC's guidance on active exploitation supports a rapid response route integrated with IT incident handling, including investigation for compromise. [Read the active exploitation guidance](#).

The wider improvement plan can capture the lasting work after urgent response is under way.

Turn each finding into a decision

Check that the finding is understood and supported. "Access management needs improvement" leaves too much interpretation. Identify which access, which systems, what evidence was seen and what could happen as a result.

Use this short structure:

- **Observation:** What was found, where and when?
- **Consequence:** What could go wrong for the business?
- **Confidence:** What is known, assumed or still to be checked?
- **Decision:** What response is proposed, and who can approve it?

Bring related findings together where they share a cause, while retaining the links to the original evidence. Several applications with overdue access reviews may need a common ownership and review process. They may also have local exposures that require separate, faster action.

If a finding is disputed, record the disagreement and the evidence needed to resolve it. Give that investigation an owner and a date. “Awaiting clarification” should have an end.

Prioritise using the business context

Discuss the credible consequence, how exposed the service is, whether exploitation or failure is already happening, and how much confidence you have in the controls. Consider commitments and deadlines, alongside dependencies and the team’s capacity.

A severity label helps organise a conversation. Keep the reasoning behind it visible. A technical score on its own cannot tell you the effect on payroll, customer delivery or the ability to recover an essential service.

Then sequence the work. An urgent containment action may be followed by a longer engineering change. A simple ownership decision may unblock several technical tasks. A new tool may need reliable asset information and a team to operate it before it can deliver the intended benefit.

NIST’s profile guidance connects gaps between current and target outcomes to a prioritised action plan, including owners, deadlines and resources. [See NIST SP 1301](#). Use that structure at the level of detail your business needs; the planning method here is a practical suggestion, not a prescribed framework timetable.

Name the delivery owner and the risk decision-maker

Give each action one accountable delivery owner, supported by named contributors. Confirm they have accepted the work and have the authority, time and access needed. “IT” is usually too broad to be useful.

Separately identify the person authorised to decide what risk the business will carry. This may be the same person in a small organisation, but the responsibilities are different. An engineer can implement a control without having authority to accept the business consequences of leaving it incomplete.

The UK Cyber Governance Code calls for senior ownership of cyber risks, an action plan aligned with risk appetite and oversight of delivery. [Read the Cyber Governance Code of Practice](#).

If work must be deferred, record the remaining exposure, reasons, interim measures, approving authority, expiry or review date, and conditions that would trigger an earlier review. A missed deadline should prompt that decision explicitly.

Write down what “done” means

Set acceptance criteria before delivery starts. They should describe the change you expect to see and the evidence needed to confirm it.

The following is an **illustrative planning record**, not a client case study or a universal remediation deadline.

Field	Example
Finding	Two sampled leavers retained access to a separately managed finance application after their departure.
Business concern	Unauthorised access to financial information and the ability to make changes after employment ends.
Immediate response	Validate the accounts and disable unneeded access; assess activity and escalate any indication of misuse.
Intended outcome	Each departure triggers removal of relevant application access, with confirmation of completion and escalation of failures.
Delivery owner	IT service owner, working with HR and the finance application administrator.
Risk decision-maker	The accountable finance executive, under the organisation's delegated authority.
Dependencies	Reliable HR notification, application ownership, an agreed removal deadline and administrator availability.
Acceptance evidence	Reconcile recent leavers against application access; test the agreed workflow and exception route; check the next operating sample for timely completion. Record coverage and unresolved exceptions.
Timing	Agree dates after urgent containment and dependency checks; record interim oversight while the lasting fix is delivered.

Use the same fields in your existing work tracker. Link the implementation tasks to the finding and risk record so the connection survives handovers.

Validate closure and keep the control working

Completion evidence should answer the original concern. A revised procedure shows that an expectation has been documented. You may also need configuration evidence, a test or a sample of normal operation to show the change is working.

For significant issues, agree a reviewer with enough independence to challenge the result. Record what was checked, the outcome, the remaining limitations and who approved closure. The NCSC's assurance guidance distinguishes confidence in implementation from confidence in continued operation. [Read the assurance guidance](#).

Give the ongoing control an owner and an appropriate checking cycle. A project can finish while the control still needs maintenance, monitoring and occasional retesting.

Make the progress meeting useful

Start with the exposures that matter most and the decisions blocking progress. Review overdue actions, failed validation, expired exceptions and changes that affect the original priority. Discuss completed work in terms of what now works and what evidence supports that conclusion.

Keep the meeting short enough to sustain. A weekly working review may suit an active improvement programme, with leadership decisions brought to an existing management forum. Adjust the cadence to the risk and pace of work.

Before agreeing the plan, check that every priority has a clear outcome, an accepted owner, a realistic sequence, a decision-maker for remaining risk and a way to prove completion. That gives the team something it can run with.

Kurosec can help assess the starting position through a [security programme review](#) and turn priorities into delivery through [security programme development](#). [Contact us](#) to discuss the work ahead.

Further reading

- [NIST SP 1301: Creating and Using Organizational Profiles](#) - moving from gaps to an action plan.
- [UK Cyber Governance Code of Practice](#) - the leadership responsibilities behind delivery.