WHITE PAPER 04 / IMPROVEMENT PLANNING

Building an Accountable IAM Improvement Roadmap

Turn assessment findings into a sequenced plan with ownership, dependencies and evidence of completion.

AIdentX Editorial | September 2026

Executive summary

An assessment can identify many valid findings and still leave a team unsure what to do next. A useful roadmap translates those findings into achievable outcomes. It explains what will change, why the change matters, which work must happen first and how the organisation will verify the result. This paper provides a practical planning method and a reusable initiative brief.

What you will take away

- Group work by a shared outcome, while preserving the original findings.
- Sequence dependencies and containment before promising delivery dates.
- Define completion as a verified change in operation.

Written for programme owners, delivery leads and risk committees.

The worked scenarios are fictional. The checklists and examples are practical editorial guidance, not customer results or a certification method.

1. Start with a business outcome

“Close all assessment findings” is a reporting ambition, not a delivery outcome. A clearer objective is that supplier access to the finance application ends when its approved business need ends. This gives the team a way to judge whether proposed tasks contribute to the improvement.

Use Cedar Vale Services, a fictional company, as an example. Its assessment identifies incomplete supplier ownership records, missing access end dates and inconsistent evidence of removal. These findings could support one improvement initiative, but they remain separate observations. Each needs a clear link to the work that will resolve it.

Before planning, review the findings for accuracy and duplication. Separate confirmed weaknesses from open questions. An investigation can be a valid first action when evidence is incomplete. It should have its own deliverable, such as an agreed account inventory or an explanation of contradictory records.

The NIST Cybersecurity Framework 2.0 uses current and target Profiles to describe cybersecurity outcomes. Comparing those states can support prioritisation; the Framework does not prescribe one implementation plan for every organisation. NIST Cybersecurity Framework 2.0.

2. Group findings without losing traceability

Group findings when they share an operational outcome, responsible team and plausible corrective action. Do not group only because the titles contain the same word. A supplier account with no owner and an application integration that ignores expiry dates may need different work even though both appear under access lifecycle management.

Finding	Proposed work	Evidence of result
No named sponsor	Reconcile supplier accounts with accountable business sponsors.	Reviewed inventory with ownership exceptions resolved or assigned.
Missing end dates	Define and implement the end-date requirement.	New requests contain authorised dates and exceptions are recorded.
Removal not demonstrated	Verify the removal process after engagements end.	Selected completed engagements link to removal records.

Keep the mapping in both directions. A reviewer should be able to open a finding and see the initiative addressing it, or open an initiative and understand the findings that justify it. If a broad programme contains several delivery tasks, assign each task an outcome that contributes to the initiative.

Avoid counting one shared action as several independent reductions in exposure. Completing an account inventory may support multiple findings, but its value comes from what it enables. The removal process may still need implementation and testing before the underlying risk changes.

3. Prioritise with explicit trade-offs

Consider the consequence of waiting, the current exposure, the effort required and any dependencies. A severe issue may need a temporary measure while a permanent fix is designed. Conversely, an apparently simple task may depend on information the organisation does not yet have. Record those constraints before turning priorities into dates.

In the example, removing access that is already confirmed as unnecessary can be handled through the authorised operational process. Building a lasting expiry workflow requires a reliable inventory and an agreed sponsor responsibility. The roadmap should distinguish immediate containment from the project that prevents recurrence.

An AI suggestion can help organise findings or propose a sequence. In AssessX, reviewers can consider AI advice during improvement planning. Check the suggested order against real staffing, change windows, application limitations and business commitments. The recommendation cannot substitute for an owner accepting delivery responsibility.

> **A practical prioritisation question**
>
> If this task slips by one month, what exposure remains, what business work is affected and which later tasks become impossible? A specific answer makes the priority easier to defend than a colour alone.

4. Write an initiative that someone can deliver

Use an initiative brief before creating a detailed schedule. The brief should be short enough for the owner to review but precise enough to prevent different interpretations of “done”. Include exclusions so the team does not silently promise a company-wide result from a limited application change.

Field	Illustrative initiative brief
Outcome	Temporary supplier access ends when authorised support work ends.
Scope	Finance application and its external support accounts.
Owner	Named finance-application service owner.

Field	Illustrative initiative brief
Dependencies	Supplier inventory; sponsor confirmation; approved change window.
Milestones	Inventory agreed; process implemented; operating sample reviewed.
Acceptance	Reviewer verifies removal against approved end dates in a new sample.
Exceptions	Each unresolved case has a justification, owner and review date.

Choose dates with the people doing the work. Record the assumption behind an estimate, especially when it relies on another team or supplier. A date without an accepted dependency is a forecast with hidden conditions. Review those conditions at each checkpoint.

Assign the verification role as well as the delivery role. Where practical, use someone who can challenge the evidence independently of the implementation. Smaller teams can document a peer or management review when full separation is not realistic.

5. Make the timeline useful

A timeline should make dependencies and decision points visible. For this fictional initiative, the first phase establishes the account population and ownership. The second changes the request and removal process. The third observes the process operating and reviews exceptions. These phases describe order, not a promised implementation duration.

Avoid scheduling every task to finish at the end of the quarter. Intermediate deliverables reveal whether the plan is progressing and allow the team to adjust before the final date. If the inventory is incomplete, show its effect on later work rather than leaving all dates green.

Track blocked work separately from completed work. A blocked task needs a decision or dependency resolved. A delayed task may need a revised forecast. Neither should be hidden by changing the due date without recording why. The history is useful when the organisation plans its next improvement cycle.

- Which milestone demonstrates a real change?
- Which earlier task must finish before this one can start?
- Who can resolve a dependency or approve an exception?
- What evidence is due at the next review, not just at the end?

6. Verify outcomes and retain the learning

Delivery completion and finding closure are different decisions. A new procedure may be published while the operational process is still untested. Keep the finding under review until the agreed evidence is available. If the verification exposes a new failure mode, update the plan instead of forcing the original closure date.

The roadmap and task views in AssessX help organise linked findings, ownership, dates and delivery work. Use them to keep the improvement understandable across security, business and delivery teams. Record the reasoning alongside the status so a new owner can continue without reconstructing the original assessment.

At the end of the initiative, compare the outcome with the starting condition. Note what changed, what evidence supports the change and what remains outside scope. Preserve any continuing exception and its review date. This creates a useful input to the next assessment rather than a closed project whose lessons disappear.

> **Before closing an initiative**
>
> Confirm that the agreed acceptance test was performed, the linked findings were reviewed, remaining exposure was assigned and the operating team knows who maintains the new process. A completed task list alone does not establish those outcomes.

References and further reading

Primary guidance used for the points cited in this paper. Examples, templates and recommended working practices are AIdentX editorial guidance. Sources reviewed September 2026.

NIST Cybersecurity Framework 2.0

https://doi.org/10.6028/NIST.CSWP.29

Put the guidance into practice

Read related articles and watch AssessX product demonstrations at www.aidentx.com/assessx/resources.