WHITE PAPER 01 / ASSESSMENT PRACTICE

Running an Evidence-Led IAM Assessment

A practical method for defining scope, asking useful questions, collecting evidence and reaching decisions that stand up to review.

AIdentX Editorial | September 2026

Executive summary

An identity and access management assessment asks a straightforward question: can the organisation show that the right people have the right access, for the right reasons? Answering it takes more than a completed questionnaire. The assessment must connect a business concern to a defined scope, testable questions, relevant evidence and accountable decisions. This paper provides a working method for that process, including an example campaign brief and a review checklist.

What you will take away

- Start with a business decision and a bounded scope.
- Ask separately about policy, implementation and actual operation.
- Keep uncertainty visible until evidence resolves it.

Written for assessment owners, security teams and business managers.

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

1. Begin with the decision

A useful assessment starts with something a business leader needs to decide. Can a new supplier receive access to the finance platform? Is the organisation ready to bring an acquired business into its identity environment? Which access weaknesses need funding this quarter? The decision determines which systems, people and controls matter. A broad request to assess all identity security usually leaves participants guessing about the level of detail required.

Identity and access management, or IAM, is the collection of processes and technology used to establish identities and control access. An assessment examines those processes. It does not itself remove an account, enforce an access policy or prove that every transaction is safe. State what the assessment can establish and what will require a technical test or a separate operational action.

> **Illustrative scenario**
>
> Cedar Vale Services is a fictional company preparing to expand supplier support for its finance application. Management wants to know whether temporary access ends when support work finishes. The assessment covers that decision, rather than every identity process across the company.

Give the campaign an owner who can resolve scope questions. Assign a business sponsor who can accept or reject the resulting recommendations. Participants provide knowledge and evidence; reviewers judge whether the answers support the conclusion. One person may hold more than one role in a small organisation, but record the responsibilities explicitly.

2. Write a scope that can be tested

Define the applications, identity populations, business processes and observation period. Include exclusions with a reason. If service accounts are excluded from a supplier-access campaign, explain where they will be assessed instead. An exclusion is a boundary, not a claim that the excluded area is secure.

Brief field	Example for Cedar Vale
Decision	Approve wider supplier support or require improvements first.
Systems and people	Finance application; external support users and their internal sponsors.
Period	Access granted or extended during the previous quarter.
Questions	Who approves access? Who records its end date? How is removal verified?

Brief field	Example for Cedar Vale
Evidence	Requests, approvals, account records and removal records for selected cases.
Review outcome	Supported finding, further evidence request or documented limitation.

Choose samples that include ordinary work and plausible failure points. For this scenario, consider a completed support engagement, an extended engagement and a sponsor who has changed roles. Explain how cases were selected. A small targeted sample can expose a weakness, but it does not establish an organisation-wide failure rate. Expand testing when the original sample reveals a pattern that needs investigation.

3. Build questions around observable behaviour

Avoid combining several controls into a single yes-or-no question. “Do you manage supplier access securely?” can hide differences between approval, expiry and removal. Ask what happens, who performs the action, when it happens and which record demonstrates it. Allow participants to say that they do not know or that a process is only partly implemented.

Use a maintained knowledge base for established questions. Where AI generates questions for the selected scope, review the output for relevance, duplication and assumptions. A question about an automated expiry mechanism may be inappropriate where the documented process is a manual removal check. The assessment should examine the actual arrangement and its adequacy, not reward a particular technology choice.

Weak question	More useful question
Is temporary access controlled?	How is the authorised end date recorded for each temporary account?
Are approvals in place?	Who approved this access, and did that person have the authority to approve it?
Does access expire?	For the selected completed engagements, what record shows when access stopped?

NIST SP 800-53A distinguishes examination, interviews and testing as assessment methods. Combining these methods helps separate a stated process from evidence of its operation. NIST SP 800-53A Rev. 5: Assessing Security and Privacy Controls.

4. Review evidence without overstating it

A policy states what should happen. A configuration export shows how a system was set up at a point in time. A ticket records a request or an action. These items answer different questions. Match each item to the claim it supports, and check its date, system, scope and origin before relying on it.

In the fictional example, a procedure says suppliers lose access when work ends. A participant confirms that the procedure is followed. Two selected cases have removal records, while a third has only an approval ticket. The fair conclusion is that removal for the third case has not yet been demonstrated. Ask for the account state or removal log before deciding whether access remained active.

Record contradictions rather than smoothing them into a favourable summary. If the ticket says access was removed but a later account export shows the account enabled, investigate the effective permissions and timestamps. A reviewer should be able to understand why an answer was accepted, returned for clarification or treated as a finding.

- Can the evidence be traced to the application and period in scope?
- Does it demonstrate the claimed action, rather than just an intention?
- Are exceptions and missing records explicitly described?
- Would a second reviewer reach the same conclusion from the recorded rationale?

5. Convert conclusions into accountable work

Write each finding in plain language: the observed condition, the evidence, the affected scope and the consequence. Distinguish a gap, such as an absent expiry check, from a risk, such as continued access after a supplier engagement ends. A missing document alone is not proof that an account was misused.

Agree the next action with the person responsible for delivering it. “Improve supplier access” is too broad. “Record an owner and end date for each in-scope supplier account, then verify removal for completed engagements” is reviewable. Define the evidence that will demonstrate completion before the work starts.

In AssessX, campaign configuration, knowledge-base and AI-generated questions, participant answers, evidence and review support this assessment workflow. The resulting risks and gaps provide a basis for improvement planning. The organisation still decides whether the evidence is adequate and whether the proposed action addresses its business exposure.

A usable closure test

For a new sample of completed supplier engagements, a reviewer can link each approved end date to the corresponding access-removal record. Any exceptions have an owner, justification and review date. This is an example acceptance criterion, not a universal sampling standard.

6. Campaign readiness checklist

Use this checklist in a short meeting before launch. Resolve disagreements about scope and evidence now, when they are easier to correct. During the campaign, keep a visible record of scope changes so the final report does not imply broader coverage than was actually achieved.

- The business decision and sponsor are named.
- Applications, identity populations, time period and exclusions are written down.
- Questions are understandable to the people expected to answer them.
- Each important claim has a proposed evidence source or test.
- Participants know how to request clarification.
- Reviewers have a route for resolving contradictory answers.
- Findings will include ownership, next action and a closure test.

At completion, report coverage as well as findings. Explain which areas were examined, which remained uncertain and which require additional work. A concise report that makes its limits clear is more useful than a confident conclusion built on incomplete answers. Keep the campaign brief for the next assessment so changes in scope can be distinguished from changes in performance.

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 SP 800-53A Rev. 5: Assessing Security and Privacy Controls

https://csrc.nist.gov/pubs/sp/800/53/a/r5/final

Put the guidance into practice

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