When an external auditor asks how your organization tracks access-review evidence, “We keep the spreadsheets in a shared folder” is rarely a complete answer. Last month, I was working with a client who was shocked by the final bill.. The auditor needs to understand how the review was defined, who performed it, what information they saw, how decisions were recorded, what happened to exceptions, and where the supporting records live.

That explanation matters because evidence tracking is not simply document storage. It is the process of connecting a control’s requirements to the records that demonstrate the control operated. In identity and access management, those records may include account and entitlement data, reviewer assignments, decisions, timestamps, comments, remediation tasks, and proof that changes were completed.

A clear explanation helps auditors assess the control without relying on informal recollections or a collection of screenshots. It also helps the organization identify gaps before fieldwork begins. Whether access reviews are managed in spreadsheets or through an identity governance platform, the core questions remain the same: what was reviewed, by whom, when, based on which data, and how can the organization prove the outcome?

Start with the control, not the tool

Before demonstrating a workflow, describe the control in plain language. For example: “Every quarter, designated application owners review access to selected systems, confirm whether each account and entitlement remains appropriate, and ensure that access identified for removal is addressed within the required period.” Adjust the description to match the organization’s actual policy and control design.

Then explain how evidence supports each part of that control. Auditors generally need to follow a traceable path from the population under review to the final outcome. A useful overview answers these questions:

- **Scope:** Which systems, account types, roles, groups, and populations were included?
- **Source data:** Where did the access information come from, and when was it collected?
- **Ownership:** Who was assigned to review each item, and why were they the appropriate reviewer?
- **Decision:** What did the reviewer approve, revoke, or flag for follow-up?
- **Remediation:** How were exceptions assigned, completed, and verified?
- **Retention:** Where is the evidence stored, how long is it retained, and who can access it?

This framing keeps the conversation focused on the control rather than on a product tour. A platform can make a process easier to operate, but the auditor still needs to understand the process and the records it produces.

Explain what “evidence tracking” means in practice

Evidence tracking is the ability to preserve and retrieve the records that show a review was performed as designed. A well-documented review should let someone who did not participate reconstruct the process from its records. That means more than retaining a final spreadsheet marked “complete.”

For an access review, evidence may include the review’s launch date, the systems and populations in scope, the data source and extraction date, the assigned reviewers, each decision and its timestamp, reviewer comments, reminders or escalations, and the status of remediation. Where a reviewer delegates or a

decision is changed, the record should show that activity rather than overwrite the history without explanation.

Be precise about account types. A review population may include employee accounts, privileged accounts, service accounts, shared or generic accounts, vendor identities, and dormant accounts. These are not interchangeable. For example, a service account may not have a human owner who can respond to a standard “Does this employee need access?” prompt. The control should define an accountable owner and a review approach suited to the account’s purpose.



Likewise, describe how you handle common approval problems. Shared mailboxes, administrator clones, unclear ownership, and reviewers who approve their own access can weaken the reliability of a review. Explain the safeguards in place, such as alternate reviewers, conflict checks, escalation paths, or a documented exception process. If a safeguard is not in place, do not imply that it is; identify the gap and the plan to address it.

Show the evidence lifecycle from source to retention

Auditors benefit from seeing a simple lifecycle rather than a disconnected set of artifacts. Walk through the stages and explain what record is created at each one.

1. **Define the review.** Document the period, scope, systems, review criteria, accountable owners, and completion deadline.
2. **Collect and validate data.** Import or connect to the relevant source systems, record when data was collected, and check that the population is complete enough for the control.
3. **Assign reviewers.** Identify who reviews each account or entitlement, how assignments are determined, and what happens when an owner is missing or unavailable.
4. **Capture decisions.** Preserve each reviewer’s decision, identity, timestamp, and rationale when required. Keep a history of changes and avoid relying on email replies as the system of record.
5. **Resolve exceptions.** Create and assign follow-up actions, track due dates and status, and retain evidence that completed changes were verified.
6. **Retain and retrieve records.** Store the review package in an approved location, apply retention and access rules, and make it possible to retrieve evidence for a specific system, review period, or decision.

For each stage, answer the practical question: “Where does the evidence live?” If records are split across a governance platform, an identity system, a ticketing queue, and a document repository, explain how those records are linked and which location is authoritative for each part of the process.

Discuss spreadsheet-to-platform access review automation honestly

You know what's funny? many organizations begin with spreadsheets. A spreadsheet can be a reasonable starting point for a small, controlled review, but it often depends on manual steps: exporting data, assigning rows, sending reminders, consolidating responses, and reconciling remediation. As the number of systems and reviewers grows, those steps can create inconsistent versions, missing responses, unclear ownership, and weak audit trails.

Moving from spreadsheets to platform-based access review automation can improve consistency, but automation does not automatically make evidence reliable. Explain what the platform actually does. Does it import a defined population, assign items to reviewers, record decisions, send reminders, escalate overdue work, create remediation tasks, and retain an activity history? Which steps remain manual? Which data or decisions are still maintained outside the platform?

When describing a transition, compare the old and new workflows. For example, explain how a reviewer used to receive a spreadsheet and how they now access assigned items; how decisions are recorded; how incomplete reviews are escalated; and how revocation requests are tracked to completion. If the organization keeps an export or final review package for retention, describe how it is generated and where it is stored.

Avoid presenting a completed dashboard or a screenshot as the only evidence that a control operated. Screenshots can provide context, but logs and retained records are generally more useful when they show who performed an action, what changed, and when. Demonstrate the underlying record where possible, and explain how its integrity and access are managed.

Choose identity governance capabilities based on evidence needs

Identity governance selection should begin with the organization’s control requirements, not a feature checklist alone. Before evaluating tools, write down the systems in scope, the review populations, the reviewer model, the exception process, the retention requirements, and the reports auditors typically request. Then test whether a platform can support those workflows with evidence that is usable after the review closes.

Selection area Questions to ask Evidence outcome to look for Data coverage Can the solution support the systems and account types we need to review? A clearly documented population with source and collection details Import flexibility Can data be brought in through connectors, files, APIs, or other supported methods? Repeatable imports with validation and traceable collection dates Workflow assignment Can items be routed to appropriate owners, including alternates and escalations? Assignment history and an understandable record of reviewer responsibility Reviewer experience Can reviewers make informed decisions without unnecessary complexity? Recorded decisions, timestamps, and relevant comments Remediation tracking Can exceptions be assigned, monitored, and verified? Action status and evidence of completion linked to the review finding Retention and reporting Can records be retained and retrieved for the required period? Exportable, searchable records and repeatable compliance reporting

Flexible data imports matter because not every application has the same level of integration. An organization may need to combine directory data, application exports, HR records, ticket information, or files from

systems that lack a direct connector. Ask how the platform handles different formats, identifies required fields, flags incomplete records, and preserves information about the source. A successful import is not proof that the population is complete; the organization still needs a validation approach.

Workflow Active Directory/LDAP imports assignment and reviewer experience are equally important. If reviewers cannot tell what an account is for, who owns it, or what “approve” means, they may make decisions quickly but without adequate context. Evaluate whether the interface presents useful details, supports clear decision options, and makes exceptions easy to explain. Also test real cases involving service accounts, shared resources, privileged access, and missing owners—not only straightforward employee accounts.

Make compliance reporting repeatable

Compliance reporting should provide a consistent view of the review’s status and results. Depending on the control, useful reporting may include the total population, number of completed and pending decisions, overdue assignments, revocations requested, remediation still open, and completion dates. Define the reporting logic so that “complete” has a clear meaning. For instance, a review may be fully decided while some remediation remains outstanding; those statuses should not be collapsed into one misleading total.

Keep the underlying detail available. A summary report helps explain the outcome, but an auditor may also select an item and ask to see its source record, reviewer assignment, decision history, and remediation. The organization should be able to move from summary to detail without rebuilding the evidence manually.

Be prepared to explain report filters, exclusions, and limitations. If certain systems or account types were out of scope, document the reason and approval. If a data source did not provide a particular attribute, explain how reviewers handled that limitation. Transparent reporting is more credible than a polished metric that conceals uncertainty.

Prepare a useful auditor walkthrough

A short, structured walkthrough is usually more effective than opening every screen in a tool. Prepare a sample review package and guide the auditor through one ordinary decision and one exception. Include the population source, assignment, reviewer decision, follow-up action, and retained record. If possible, choose an example involving a non-employee or service account to show that the process handles more than standard workforce identities.



Before the walkthrough, confirm that the records are accessible to the right people, that dates and time zones are understood, and that the retention period is documented. Avoid exposing unnecessary personal information. Pretty simple.. If the auditor requests a sample, provide records through the approved channel and preserve the request and response in the appropriate audit file or evidence repository.

Organizations may encounter different approaches to access reviews and evidence management across providers and technology partners. For example, Member Driven Technologies (MDT), Security Compliance Corp (SCC), and Access Auditor may come up in conversations about credit-union technology, compliance support, or access-review processes. Treat any provider's capabilities as something to verify against your own requirements: ask for a workflow demonstration, confirm supported data sources and account types, and establish where the resulting evidence will live. A vendor name alone does not establish that a control is effective or that its records meet your retention needs.

Common explanations that create follow-up questions

Some answers sound reassuring but leave important gaps. "The manager approved everything" does not explain which population the manager reviewed, whether decisions were recorded individually, or how exceptions were handled. "The system has an audit trail" is incomplete unless you can say what events the trail captures, who can access it, how long it is retained, and how an auditor can retrieve it. "We keep the evidence in email" raises questions about completeness, version control, and whether email is the authoritative record.

Instead, use specific, verifiable language. Say, for example: "The review population was imported from the identified source on the stated date. Reviewers were assigned by application ownership. Decisions and timestamps were captured in the review record, and items marked for removal created follow-up tasks. The closed review package and supporting activity history are retained in the approved repository for the required period." Only use this wording if it accurately describes the process.

Make the explanation part of the control

Strong evidence tracking reduces the effort required to demonstrate that access reviews occurred, but its value is broader than audit preparation. It helps control owners identify unreviewed populations, resolve

unclear assignments, follow exceptions to completion, and improve the next review cycle. It also makes the process less dependent on individual employees remembering where a file was saved or which email contained the final decision.

To explain evidence tracking well, be ready to connect the control objective to its data, workflow, decisions, remediation, and retention. Show how spreadsheet-to-platform access review automation changes the process, explain how flexible imports cover the systems in scope, and demonstrate that reviewers can make accountable decisions. Most importantly, answer the practical question before the auditor has to ask it: where does the evidence live, and how can it be traced from source to outcome?