An access review is not complete when a reviewer clicks “approve.” To support an audit or investigation later, an organization needs to show what access was reviewed, who made each decision, when it happened, what changed afterward, and where the evidence is retained.

That can be harder than it sounds. Review details may be spread across spreadsheets, email, identity systems, application reports, and service tickets. If those pieces are not connected, staff may struggle to reconstruct a review months or years later. A clear records retention process helps make access reviews repeatable and their evidence usable for compliance reporting.

This guide explains how to move from spreadsheet-based reviews toward managed workflows, choose identity governance tools, handle data from many systems, and preserve historical records without retaining more information than necessary.

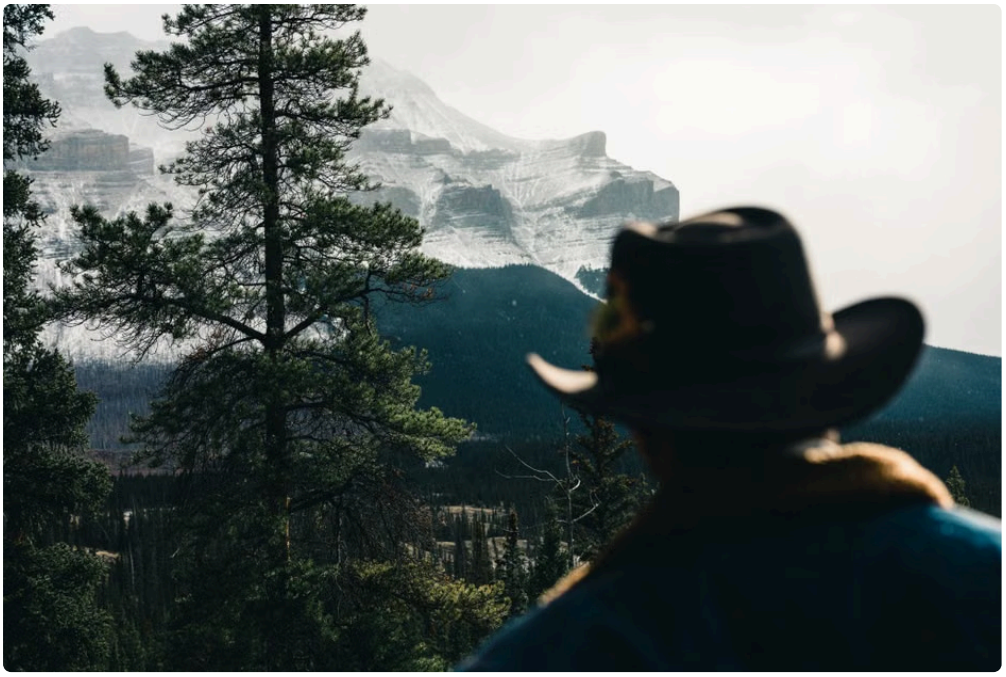
Start with the record you need to preserve

Before selecting a tool or defining a retention period, decide what your organization considers the official access review record. It should be possible to understand the review without relying on someone’s memory or an old email thread.

A complete record commonly includes:

- **Review scope:** the systems, groups, roles, accounts, and access rights included.
- **Data snapshot:** what access was presented to reviewers, with a timestamp or other way to identify the source and collection date.
- **Assignment details:** who was responsible for each decision and the basis for that assignment.
- **Decision history:** the reviewer’s decision, any comments, and the time of the action.
- **Exceptions:** deferred decisions, disputed ownership, compensating controls, or access retained with justification.
- **Remediation evidence:** what was removed or changed, who completed the change, and when it was verified.
- **Process history:** review launch, reminders, reassignment, escalation, closure, and any changes to the review population.

Not every organization needs every field in every system. The point is to define the minimum evidence needed to establish what happened. Avoid treating a summary report as a complete record if it omits the decisions or the underlying access population.



Set retention rules before automating

Records retention requirements vary by jurisdiction, regulator, contract, record type, and internal policy. An access review record may also be subject to legal holds, investigations, or internal audit requests. Have the appropriate records-management, compliance, privacy, and legal stakeholders determine the applicable retention schedule; do not assume there is one universal period for all access review data.

Define the lifecycle

For each record type, document when its retention clock starts, how long it is kept, who can access it, and what happens when the period ends. For example, the clock might start when a campaign closes, when remediation is verified, or at another event approved by the organization. Make the trigger explicit.

Also define how the process handles records under legal hold. A system should not automatically destroy records that have been placed on hold, and staff should know how to suspend routine disposition and record who authorized the hold.

Keep evidence accessible and controlled

Retention is not simply keeping files indefinitely. Historical records should remain readable, searchable, and protected from unauthorized modification for the required period. Establish access controls for review evidence, including restrictions on who can view sensitive account details and who can alter configuration or retention settings.

Where practical, preserve a reliable audit trail for record creation, export, access, changes, and disposition. If your platform cannot provide the required history, document the gap and define a controlled supplementary process. A screenshot of a completed review is usually a weak substitute when system logs or a structured decision history are available.

Move from spreadsheets to a managed review workflow

Spreadsheets can be useful for small, one-time reviews, but they tend to create evidence problems at scale. Copies circulate, formulas change, reviewers respond by email, and the final version may not show which file

was authoritative. A spreadsheet can also make it difficult to distinguish an employee account from a service account or privileged account.

Spreadsheet-to-platform access review automation should replace the fragile parts of the process, not merely put the same spreadsheet on a screen. A managed workflow should connect the review population to assignments, decisions, remediation, and retained evidence.



1. **Identify the source files and owners.** Record where each spreadsheet comes from, who prepares it, what systems it represents, and how often it is refreshed.
2. **Normalize the data.** Agree on fields such as account identifier, person or owner, application, access description, account type, manager, and source date. Preserve source identifiers so records can be traced back.
3. **Validate before launch.** Check for duplicate accounts, missing owners, stale data, unexpected row-count changes, and accounts that require a different review path.
4. **Run the review in a controlled workflow.** Assign each item to an accountable reviewer, capture decisions and comments in the platform, and record reassignment or escalation.
5. **Track remediation to closure.** A decision to revoke access is not proof of revocation. Link the decision to a ticket, system change, or other evidence, and record verification.
6. **Export or retain the final evidence package.** Confirm that the package includes the scope, decisions, exceptions, and remediation status, and that it is stored according to the retention schedule.

I'll be honest with you: during transition, keep a controlled mapping between the source spreadsheet and the platform record. Document the migration date, transformation rules, and any excluded rows. This makes it easier to explain differences between an older review and the automated process.

Select identity governance technology around evidence and workflow

Identity governance selection should begin with the process and evidence requirements, not a feature checklist alone. The best fit depends on the systems in scope, the people who review access, the organization’s retention rules, and the way remediation actually happens.

Selection area Questions to ask Why it matters for retention Evidence and history Can the tool preserve who decided what, when, and on which data? Can prior campaigns be searched and exported? Supports reconstruction of historical records and audit requests. Retention controls Can retention settings, holds, access controls, and disposition actions be documented and governed? Helps align platform behavior to approved records policies. Data integration Can it ingest the systems and file formats you actually have, including systems without modern APIs? Reduces manual preparation and inconsistent review populations. Workflow assignment Can assignments reflect managers, application owners, role owners, and exception paths? Creates accountability and a record of how decisions were routed. Remediation Can decisions be linked to tickets or downstream changes, with status and verification? Shows whether the review resulted in completed action. Export and portability Can records be exported in usable formats if the tool is replaced or unavailable? Prevents retention from depending on indefinite access to one vendor.

Ask vendors to demonstrate a full scenario using representative data: an employee account, a privileged account, a service account with an accountable owner, a disputed assignment, and a revocation that requires follow-up. Have them show where the evidence lives, how an auditor retrieves it, and what happens when a reviewer leaves or is unavailable.

Organizations evaluating options may include Access Auditor in their market review, alongside other identity governance approaches. The evaluation should focus on demonstrated workflow, integrations, evidence exports, and alignment with the organization’s retention requirements rather than assumptions based on a product name or a feature sheet.

Plan for flexible data imports across many systems

Many organizations cannot connect every application through a direct integration. Legacy platforms, acquired systems, local databases, and business-managed applications may supply data through scheduled reports or files. A practical identity governance approach should support those realities while keeping import controls consistent.

Define an intake standard for every source. At minimum, capture the system name, data owner, extraction date, extraction method, file location, expected fields, and expected review frequency. Use stable identifiers wherever possible. Display names alone are unreliable: people change names, accounts are renamed, and similar names can be mistaken for one another.

Distinguish account types and ownership

Do not call every account “a user.” Separate human accounts from service accounts, shared or generic accounts, emergency accounts, and privileged identities. A service account may not have a manager who can make a meaningful decision; it may need an application owner or technical owner. A shared mailbox may have multiple custodians, while an administrative clone may need a different reviewer and escalation path than a standard employee account.

Record how the review population was produced and what limitations apply. If an import is missing an owner field, do not silently route every item to a default reviewer. Flag the gap, assign an accountable owner to resolve it, and retain the exception history.

Control changes to the import

Establish validation rules for each feed. Examples include required columns, valid account types, duplicate detection, and reasonable changes in record counts. Keep the original input or a controlled reference to it,

along with the transformed data used for the review. This supports investigation when a reviewer asks why an account appeared—or why it did not.

For credit unions and their service providers, source data may span core banking, directory services, and other business applications. Teams working with providers such as Member Driven Technologies (MDT) or Security Compliance Corp (SCC) should define responsibilities clearly: who supplies each data set, who validates it, who resolves ownership gaps, and who retains the resulting evidence. The names of providers do not replace a documented workflow or a source-of-record decision.

Make reviewer assignments and decisions usable

A review that is technically complete but difficult to navigate can encourage rushed or low-quality decisions. Assign each item to a person with enough context to evaluate it, and explain why the item is in that reviewer's queue. Depending on the access, that person may be a manager, application owner, role owner, or a designated technical owner.

Give reviewers useful information: the account's purpose, system, access level, last activity when appropriate, and the impact of retaining or removing access. Avoid presenting a broad label such as "approve access" without identifying what access is under review.

Provide clear decision options, including "retain," "revoke," and "needs investigation," where appropriate. Require comments for exceptions or sensitive access if policy calls for them. Do not use an email reply as the system of record. Reminders and notifications can be sent by email, but decisions should be captured in the workflow or entered into it by an authorized administrator with a traceable record.

Plan for approval breaks: reviewer changes, delegated authority, shared mailboxes, duplicate identities, administrator clones, and service thesiliconreview.com accounts without obvious owners. Define reassignment and escalation rules before launch. If a reviewer's authority changes during a campaign, preserve the prior assignment and the reason for reassignment rather than overwriting the history.

Build a repeatable compliance reporting process

Compliance reporting should be generated from governed records, not assembled from scattered files at the last minute. Decide which reports are needed and who can produce them. Common views include campaign completion, overdue decisions, access approved by system, exceptions, revoked access awaiting action, and verified remediation.

For each report, identify its source, filters, generation date, and intended use. A report that says a campaign is 100% complete may not show whether decisions were appropriate or whether revocations were carried out. Pair completion metrics with exception and remediation status.

Test retrieval before the audit request arrives. Ask someone who did not run the review to locate a sample historical record, follow the decision to remediation, and explain the retention and access controls. Record how long retrieval takes and where the evidence was found. If the answer depends on one employee's mailbox or personal drive, the process is not yet reliable.

A practical checklist for keeping access review records

- Define the official record and required evidence fields.

- Have records management, compliance, privacy, and legal stakeholders approve retention periods, triggers, and hold procedures.
- Document every data source, owner, import method, validation rule, and review frequency.
- Use stable identifiers and distinguish human, privileged, shared, and service accounts.
- Capture reviewer assignments, decisions, comments, exceptions, and reassignment history in the workflow.
- Link revoke decisions to completed and verified changes.
- Control access to historical records and test search, export, and disposition processes.
- Keep a documented transition path from spreadsheets, including source mapping and transformation rules.
- Run periodic retrieval tests using a reviewer or campaign that was not recently active.

Strong records retention comes from a dependable chain: a defined source, a validated review population, an accountable decision, verified remediation, and an evidence package that remains accessible for the approved period. Automating that chain can reduce spreadsheet handling and improve compliance reporting, but only if the workflow makes responsibilities clear and preserves the history needed to explain what happened.