Access reviews are easy to describe and harder to run well. A review may involve employees, privileged accounts, service accounts, applications, and permissions spread across multiple systems. Reviewers need enough context to make informed decisions, managers need a clear path to complete their assignments, and audit teams need evidence that shows what happened—not just a collection of “approved” replies.



For Member Driven Technologies (MDT), a credit union service organization supporting financial institutions and their technology environments, those requirements make the review process especially important. A spreadsheet-based approach can get a review started, but it can also create avoidable work: gathering data, assigning reviewers, tracking overdue responses, reconciling changes, and storing evidence. A platform such as Access Auditor, from Security Compliance Corp (SCC), can help organize these activities into a repeatable workflow.

This is not simply a story about replacing spreadsheets with software. It is about designing a process in which data, decisions, follow-up, and evidence remain connected from the start of a review to its close.

Why user access reviews become difficult to manage

A user access review asks the right people to confirm whether accounts and entitlements remain appropriate. That sounds straightforward until the review spans several systems and account types. A credit union may need to review Active Directory access, application roles, infrastructure permissions, and accounts in core banking or other business platforms. Some records belong to employees; others belong to service accounts, administrators, vendors, or shared mailboxes.

Those distinctions matter. A manager may be able to confirm an employee’s job responsibilities, but may not know why a service account has a particular permission. A shared mailbox may have multiple delegates, while an administrative clone may need to be reviewed against a separate control. Treating every record as “a user” can obscure who owns the access and who is qualified to approve it.

Spreadsheet reviews often put the burden of keeping those details straight on the coordinator. That person may export data from different sources, normalize names and identifiers, split the workbook into reviewer

assignments, and later combine the results. Each manual step creates an opportunity for missed records, inconsistent decisions, or uncertainty about which file is current.

Before Access Auditor: the spreadsheet-led workflow

In a spreadsheet-led process, the review usually begins with data collection. An analyst requests exports from system owners or administrators, often in different formats. One file may use employee IDs, another may use email addresses, and a third may identify accounts by a local system name. The analyst has to determine how records relate before the review can be assigned.

Once the data is prepared, the coordinator distributes review sheets. Reviewers may receive files by email, make decisions in the workbook, and return them when complete. The coordinator then tracks who has responded, follows up on overdue assignments, resolves ambiguous answers, and consolidates the final results.



This approach can be workable for a limited review. Its weak point is not that spreadsheets are inherently bad; it is that a spreadsheet is usually being asked to perform several jobs at once. It acts as a data repository, assignment tool, status tracker, decision record, and evidence package. Email becomes the informal workflow around it, even though email replies are not a reliable system of record for the review.

Review activity Common spreadsheet-led challenge What a platform-based process can improve Data preparation Manual cleanup of different exports and identifiers Repeatable imports and a consistent review population Assignment Separate files, email instructions, and unclear ownership Visible assignments and reviewer-specific work queues Follow-up Manual reminders and status tracking Central progress tracking and structured follow-up Evidence Multiple workbook versions and scattered email replies Decisions and review history retained with the review record

After Access Auditor: a more structured review cycle

With Access Auditor, the process can shift from assembling and chasing files to managing a defined review cycle. The organization still needs to decide what data belongs in scope, who should review it, and what decisions are acceptable. The difference is that the platform can provide a place to organize the imported records, route assignments, capture decisions, and retain review history.

A practical workflow starts with the review population. The team identifies systems and account types to include, imports the relevant access data, and checks the resulting records before assignments go out. Reviewers receive work based on the defined ownership model. They can make decisions in the review workflow rather than returning a separate spreadsheet, while administrators monitor completion and handle exceptions.

When a reviewer identifies access that should be removed or changed, the review decision should not be confused with proof that the change was completed. A sound process records the reviewer's decision and then tracks remediation through the organization's established change or service-management process. At closeout, the review record should make it possible to see what was reviewed, who made each decision, when it was made, and how exceptions were handled.

A sample end-to-end workflow

1. **Define the review.** Set the review period, systems in scope, account types, decision options, due dates, and escalation path.
2. **Import and validate data.** Load source records, check for missing owners or identifiers, and resolve duplicate or ambiguous entries before launch.
3. **Assign reviewers.** Route records to managers, application owners, or other qualified reviewers according to the review's ownership rules.
4. **Complete decisions.** Reviewers confirm, revoke, or flag access for follow-up, using available context to make a defensible decision.
5. **Monitor completion.** Coordinators review progress, follow up on outstanding assignments, and address exceptions without rebuilding the status report from separate files.
6. **Track remediation and close.** Send removal or change decisions to the appropriate operational workflow, verify completion as required, and retain the review evidence.

Flexible data imports across many systems

Identity governance selection criteria should include how a platform handles the organization's actual data—not just the systems with the cleanest integrations. Credit unions and their service providers often work with a mix of directories, applications, infrastructure platforms, and business systems. Their exports may differ in column names, account identifiers, role descriptions, and the level of detail they contain.

Flexible import options can help teams bring those records into a consistent review process even when source systems vary. That flexibility is valuable when a system does not provide a direct connector or when an organization needs to include a one-time data source. It also makes it possible to start with a focused review and expand coverage over time.

Import flexibility does not remove the need for data governance. Before a review begins, thesiliconreview.com teams should establish how accounts are identified, how ownership is assigned, and how special account types are handled. For example, an employee account may be matched to a directory identity, while a service account may require an application owner and a documented business purpose. If the source data does not identify an accountable reviewer, that gap should be addressed rather than hidden by the import.

When evaluating a platform, ask how it handles malformed records, duplicate entries, missing attributes, and changes to a source file between review cycles. Ask whether administrators can validate the population

before launch and whether imported data can be traced back to its source. These details often determine whether flexible imports save time or simply move manual cleanup to a different screen.

Workflow assignment and reviewer experience

Reviewer experience is a control consideration, not just a usability preference. If reviewers cannot tell what they are responsible for, what each permission means, or how to record a decision, completion may be slow and inconsistent. A well-designed workflow gives each reviewer a manageable assignment, clear instructions, relevant access details, and a straightforward way to flag uncertainty.

Assignment rules should reflect real ownership. Managers may review employee access, application owners may assess roles within a system, and designated technical owners may review service accounts or privileged access. For records with shared responsibility, the process should make that responsibility explicit. Sending every item to one manager because that person is easy to identify is not the same as establishing appropriate review accountability.

Centralized progress tracking also changes the coordinator's job. Instead of compiling replies and asking who has returned a workbook, the coordinator can focus on records that are overdue, disputed, or missing an owner. Reminders and escalations should be part of the defined workflow, with a clear record of status and follow-up. Email can notify people, but the decision and its supporting history should remain in the review system.

Audit evidence retention: keep the decision and its context

Audit evidence retention is stronger when the evidence is produced as part of the process rather than assembled after the fact. A final spreadsheet may show a list of approvals, but it may not explain who changed a decision, when the review was completed, which data was presented to the reviewer, or what happened to access marked for removal.

A useful review record should preserve the population reviewed, reviewer assignments, decisions, timestamps, comments or exception details where relevant, and the review's status. It should also support the organization's process for connecting access decisions to remediation records. The specific evidence retained should align with internal policy, regulatory obligations, and the organization's audit requirements.

Before selecting a tool, ask the question that often gets missed in a product demonstration: **Where does the evidence live?** Confirm how review history is stored, who can access it, how it can be retrieved for an audit, and how long it is retained. If system logs can provide reliable evidence, use them where appropriate; screenshots are a poor substitute when authoritative records are available.

Choosing an identity governance platform

For MDT and the credit unions it supports, selecting an identity governance platform should begin with the operating model. The goal is not to buy the longest feature list. It is to make recurring controls more consistent and easier to demonstrate across the systems and account types that matter.

- **Data coverage:** Can the platform handle imports from the systems in scope, including varied file formats and account types?
- **Review ownership:** Can assignments reflect managers, application owners, technical owners, and other accountable reviewers?

- **Reviewer workflow:** Can people understand their assignments, make clear decisions, and flag exceptions without relying on a separate workbook?
- **Evidence and reporting:** Can the organization retrieve review history and show completion, exceptions, and follow-up?
- **Operational fit:** Does the process connect review decisions to existing remediation and change workflows?
- **Administration:** Can the team configure repeatable reviews and manage data quality without creating a large manual burden?

MDT's environment and each member institution's environment may have different source systems, responsibilities, and review schedules. That makes a practical evaluation more useful than a generic demo. Test the platform with representative data: include a standard employee account, a privileged account, a service account, and a record with incomplete ownership. Then walk through import, assignment, decision-making, exception handling, and evidence retrieval.

What changes—and what still requires judgment

Moving from spreadsheets to Access Auditor can reduce the administrative effort involved in coordinating user access reviews and give teams a more consistent place to manage decisions. It can make assignments more visible, support flexible data intake, and improve audit evidence retention by keeping review activity connected to the review itself.

Automation does not decide whether an access grant is appropriate. Reviewers still need context, owners still need to be accountable, and administrators still need to investigate unusual or incomplete records. A platform cannot compensate for an undefined review policy or a data source that omits important account details.

The strongest "after" process is therefore a combination of technology and clear operating rules: define the population, assign the right reviewers, make decisions in a traceable workflow, follow remediation to completion, and retain evidence where it can be retrieved. For Member Driven Technologies and the institutions it serves, that is the practical value of moving beyond spreadsheet coordination: not simply fewer files, but a review process that is easier to run, understand, and substantiate.