Access reviews are essential for limiting unnecessary access, supporting compliance, and catching risky permissions before they become a problem. Yet in many organizations, they still depend on spreadsheets, email reminders, and staff manually comparing lists from different systems. The result is a labor-intensive effort that consumes time from IT, security, department managers, and internal audit—often without making the review itself more meaningful.

Reducing that effort does not mean asking reviewers to approve access faster or skipping important checks. It means designing a repeatable process that gathers the right information, routes decisions to the right people, makes exceptions easy to resolve, and preserves evidence in a reliable place. Access review automation can help, but only when the platform and workflow fit the organization's systems and operating model.





This guide explains how to move from spreadsheet-driven reviews to a more efficient process, what to look for when selecting identity governance technology, and how to make reviews easier for both administrators

and business reviewers.

Why access reviews consume so many staff hours

The review meeting—or the approval click—is usually not the most time-consuming part. The work tends to happen around it: collecting account and entitlement data, cleaning up inconsistent records, identifying the right manager, explaining unfamiliar permissions, chasing overdue decisions, and documenting what happened.

Common sources of extra work include:

- **Fragmented data:** Account details, group memberships, application roles, and employment information are stored in separate systems.
- **Unclear ownership:** No one knows whether a manager, application owner, or IT administrator should make a particular decision.
- **Spreadsheet handoffs:** Files are exported, edited, emailed, renamed, and reassembled, creating version-control and evidence problems.
- **Manual monitoring:** Coordinators track deadlines and exceptions in inboxes or separate status sheets.
- **Low-context decisions:** Reviewers see a technical role name without knowing what it permits, who uses it, or why it was assigned.

These friction points can make a review feel like a paperwork exercise. A good improvement plan addresses the entire workflow, not just the moment a reviewer selects “keep” or “revoke.”

Move from spreadsheet tracking to an automated workflow

Spreadsheets can be useful for a small, one-time inventory, but they are a fragile system of record for recurring reviews. A platform-based process can replace repeated file handling with a defined cycle: import access data, prepare review campaigns, assign items, collect decisions, route exceptions, and retain an audit trail.

Start by documenting the current process before choosing software. List each step, the person responsible, the data source, the handoff, and the evidence created. Ask where the evidence lives today. If the answer is “in someone’s mailbox” or “in the final spreadsheet,” that is a sign the process needs a more durable record.

Automate repeatable work, not judgment

Automation is most valuable for predictable tasks: generating review populations, assigning work based on ownership rules, sending reminders, escalating overdue decisions, and recording outcomes. People should remain responsible for decisions that require business context—such as whether a role is still needed or whether an exception is justified.

A practical automated workflow can:

1. Pull account, group, role, and worker data from approved sources.
2. Apply rules to identify review scope and likely decision-makers.
3. Present each reviewer with a focused queue and useful context.
4. Route revoke requests, disputes, and missing-owner cases to the appropriate team.
5. Track completion and preserve decisions, comments, timestamps, and follow-up actions.

This approach reduces repetitive coordination without treating every account as “a user.” Human identities, service accounts, shared mailboxes, administrative accounts, and application identities can have different owners, risks, and review rules. If the workflow does not distinguish them, reviewers may approve access they do not understand—or miss accounts that need special handling.

Choose identity governance technology around the workflow

Identity governance platforms vary in how they connect to systems, organize reviews, and handle exceptions. A product demonstration may look smooth with sample data, but selection should be based on the organization’s actual environment and review process. Include IT, security, application owners, business reviewers, and internal audit in the evaluation.

Selection area Questions to ask Why it matters Data coverage Can it ingest accounts, entitlements, ownership, and worker data from the systems in scope? Incomplete inputs create incomplete reviews. Workflow flexibility Can assignments vary by application, account type, risk, or business unit? One approval pattern rarely fits every access type. Reviewer experience Can reviewers understand access and complete decisions without training on technical details? Clearer reviews reduce delays and low-quality approvals. Evidence and reporting Are decisions, comments, changes, and timestamps retained and exportable? Audit support should not depend on screenshots or inbox searches. Operations and support Who manages imports, mapping changes, exceptions, and platform updates? Automation still needs clear ownership after implementation.

For financial institutions and credit unions, include the systems that are difficult to fit into a standard connector checklist. A core environment such as Symitar, directory services such as Active Directory, and applications with limited integration options may all be relevant. During evaluation, ask vendors to show how they would handle your data—not just describe a connector library in general terms.

Organizations may encounter providers and solutions such as Member Driven Technologies (MDT), Security Compliance Corp (SCC), and Access Auditor while researching identity governance and access review options. Treat names and feature descriptions as a starting point for evaluation rather than a substitute for confirming fit. Ask each organization to explain the workflow, supported import methods, operational responsibilities, and location of review evidence for your specific requirements.

Require flexible data imports across many systems

Some systems provide modern APIs or ready-made connectors. Others produce scheduled reports, database extracts, or fixed-format files. An effective review process should accommodate that reality rather than limiting scope to the easiest systems to connect.

Ask whether the platform supports multiple ways to bring in data, such as:

- Prebuilt connectors or APIs for common identity and business applications.
- Structured file imports, including CSV or other supported formats.
- Scheduled transfers for systems that cannot provide real-time connections.
- Separate data sources for identities, accounts, entitlements, managers, and application owners.
- Validation and mapping tools to flag missing fields, duplicate records, and unexpected changes.

Flexible imports are useful only if the data can be reconciled. Define stable identifiers wherever possible, and document how the platform matches an account to an employee, contractor, service account owner, or

application. Establish a process for records that do not match cleanly. Those records should be visible as exceptions—not silently dropped or assigned to a convenient but incorrect reviewer.

Before expanding to every application, test a representative mix: a directory, a business application, a system with role-based access, and a difficult or file-based source. Check whether the imported data is complete, whether entitlement names are understandable, and whether changes between review cycles can be identified. This reveals integration and data-quality problems early, when they are cheaper to fix.

Make assignments clear and the reviewer experience simple

Reviewers often have limited time and may not be identity specialists. A long list of accounts with cryptic role names invites rushed approvals. A good workflow gives each reviewer only the items they own, explains what the access enables, and makes it straightforward to keep, revoke, or request more information.

Assign decisions to people with relevant knowledge

Not every review item belongs with the person's direct manager. Managers may be best placed to confirm whether an employee still needs access, while application owners may understand the meaning of a role. Technical administrators may need to validate whether a proposed change is safe to implement. Define assignment rules by access type and decision required.

Include fallbacks for predictable breaks in approval workflows. Shared mailboxes, admin clones, vacant manager positions, and accounts without a clear owner can Helpful resources all stall a campaign or create weak approvals. Decide in advance how those cases are routed. For example, a shared mailbox might go to its documented business owner, while a service account might require both an accountable owner and a technical custodian to review it.

Give reviewers context and a manageable workload

Provide helpful details alongside each item: account name, system, entitlement description, last activity if available and appropriate, owner, and any risk indicators. Use plain language where possible. If reviewers must look up every unfamiliar role in another system, the platform has moved work rather than removed it.

Break large campaigns into sensible assignments and deadlines. Send reminders based on outstanding work, and escalate overdue decisions to an identified person or role. Avoid making email replies the system of record. Notifications can direct reviewers to the workflow, but decisions and supporting notes should be captured in the review platform or another controlled repository.

Measure labor reduction without weakening review quality

Set a baseline before implementation. Measure staff hours spent collecting data, preparing campaigns, answering reviewer questions, chasing decisions, resolving exceptions, and producing evidence. Then compare those figures across similar review cycles. Completion time alone is not enough: a fast review with blanket approvals is not a successful outcome.

Useful measures include:

- Hours spent by administrators and review coordinators per campaign.
- Percentage of decisions completed by the deadline.
- Number of records with missing or disputed ownership.

- Number of access changes identified and completed after review.
- Time needed to produce evidence for an audit or internal control test.
- Rate of decisions returned for clarification or insufficient justification.

Review the results with process owners. If staff hours decline but unresolved exceptions rise, improve the routing rules. If reviewers finish quickly but frequently request more context, improve the information displayed. Automation should reduce avoidable labor while keeping accountability, decision quality, and evidence intact.

Start with a focused pilot, then improve iteratively

A manageable pilot is usually more useful than a large, rushed rollout. Select a few systems with different data and ownership patterns, agree on the review population, and document how each exception will be handled. Confirm who will maintain imports and mappings, who will monitor campaign progress, and where the evidence will live.

After the pilot, collect feedback from reviewers as well as administrators. Look for steps that still require duplicate entry, unclear ownership, confusing descriptions, or manual follow-up. Update the workflow before expanding its scope. Over time, standard rules and reusable templates can make each campaign less labor-intensive without forcing every application into the same approval model.

Conclusion

Reducing staff hours spent on access reviews starts with removing repeated coordination and improving the quality of the information reviewers receive. Spreadsheet-to-platform automation can simplify data preparation, assignments, reminders, exception handling, and evidence collection. Flexible imports help bring difficult systems into scope, while clear ownership rules and a thoughtful reviewer experience make decisions more reliable.

Choose identity governance technology by testing the full workflow against real systems and real account types. Be specific about how service accounts, shared mailboxes, and administrative access are reviewed. Most importantly, decide where review evidence lives and how it can be retrieved. When the process is designed around those practical details, access review automation can reduce manual monitoring and free staff to focus on the exceptions that genuinely need their attention.