Access reviews are one of the most visible IAM controls—and one of the easiest to turn into a box-checking exercise. A spreadsheet is emailed to a manager, a few cells are updated, and the file is saved somewhere for audit. The process may produce a completed review, but it does not necessarily show that the right access was reviewed by the right person, that exceptions were resolved, or that changes were made.

For critical applications, a strong review process connects business decisions to verifiable action. It identifies who and what can access an application, gives knowledgeable reviewers a clear assignment, records their decisions, and tracks approved changes through completion. This guide explains how to build that process, move from spreadsheet-based reviews toward automation, and evaluate identity governance tools without losing sight of the evidence.

## Why Critical Applications Need a Different Level of Attention

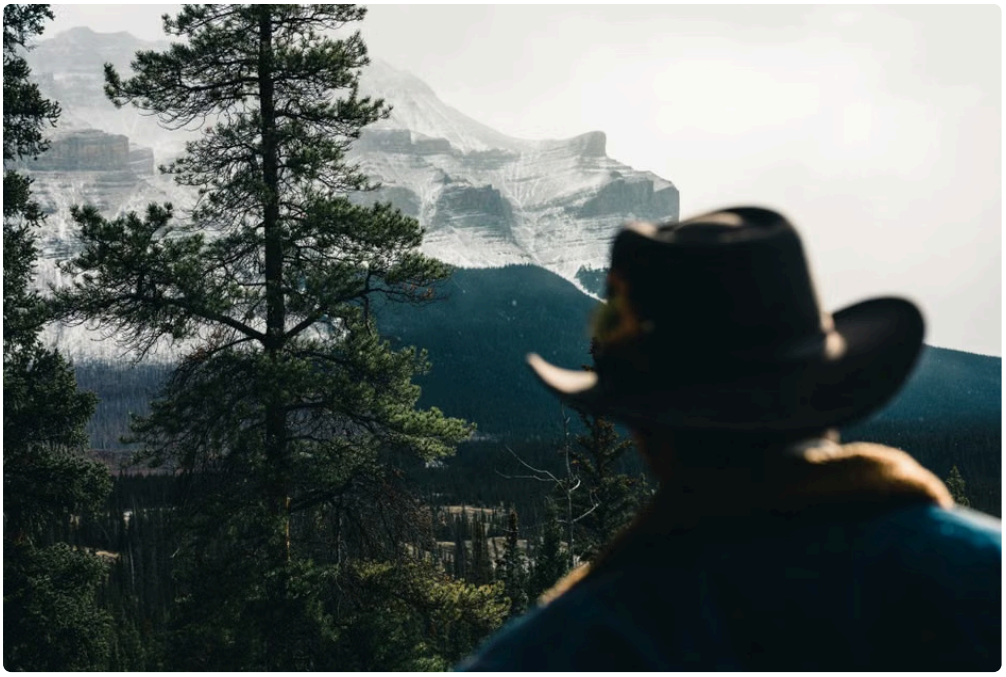
Not every application presents the same risk. A low-impact collaboration tool may warrant a lighter review than a core banking platform, payment system, identity provider, or application that stores sensitive member or customer information. The review cadence and depth should reflect the consequences of inappropriate access.

Start by defining what “critical” means for your organization. Consider business impact, data sensitivity, regulatory obligations, privileged functionality, and whether the application supports essential operations. Include applications hosted by a third party as well as those managed internally. A vendor-hosted platform can still represent a significant access risk if it processes sensitive data or connects to internal systems.

Also review more than employee accounts. Critical applications may contain:

- Employee and contractor accounts, including accounts belonging to people who have changed roles.
- Privileged or administrator accounts, which may have broad permissions or the ability to change configurations.
- Service accounts and integration identities used by applications, scheduled jobs, or system connections.
- Shared or generic accounts, which can make it difficult to identify who performed an action.
- Vendor and support accounts, including access that was intended to be temporary.
- Inactive, duplicate, or orphaned accounts that no longer have a clear business owner.

Calling every account “a user” can obscure important differences. A manager may be qualified to confirm an employee’s job access but may not know whether a service account is still required. Build account type and ownership into the review data, and route each type to an appropriate person.



## Define the Review Before Choosing a Tool

Technology cannot compensate for an unclear review. Before selecting a platform or automating a spreadsheet, document the process you need it to support. A practical review has a defined scope, a reliable source of access data, accountable reviewers, clear decision options, and a way to confirm that approved removals or changes were completed.

### Set scope and frequency by risk

List the critical applications and identify the access being reviewed in each one. A review might cover application roles, group memberships, entitlements, administrative privileges, or some combination. Be specific: “review access to the finance application” is less actionable than “confirm each account’s role, privileged status, and business need.”

Set review frequency based on risk and applicable internal requirements. Some access may be reviewed quarterly, while other access can be reviewed less frequently. Define additional triggers for event-driven reviews, such as a role change, a system acquisition, a major configuration change, or a security incident. The important point is to make the schedule intentional and repeatable.

### Identify accountable reviewers

Reviewers should have enough context to make an informed decision. Managers can often confirm whether an employee still needs access, but application owners may be better positioned to assess whether a particular role is appropriate. Data owners can help assess access to sensitive information. Privileged and service accounts may require review by a technical owner together with a business owner.



Establish a fallback and escalation path before launching the campaign. A review assigned to someone who has left the organization—or to a shared mailbox that no one monitors—can stall or be completed without meaningful oversight. These are common approval failure points. Assign a named owner or documented delegate, and make reassignment visible in the review record.

## Build a Spreadsheet Process That Can Be Controlled

Many organizations begin with spreadsheets because they are familiar and easy to distribute. A spreadsheet can be a useful input or interim method, but email replies and scattered file copies should not become the system of record. Without controlled assignment, status tracking, and change evidence, it is difficult to prove who reviewed what and what happened afterward.

If you use spreadsheets, standardize the structure. Include fields such as:

- Application and environment.
- Account name, account type, and unique identifier.
- Person or service owner associated with the account.
- Role, group, entitlement, or privilege being reviewed.
- Last sign-in or other relevant activity information, where available and appropriate.
- Reviewer, decision, comments, and decision date.
- Remediation owner, due date, completion status, and evidence reference.

Control the file version, restrict access to it, and record when assignments are issued and returned. Avoid treating an unchecked cell as an approval. Require a deliberate decision such as retain, modify, or revoke, with comments when the choice needs explanation. Define how incomplete rows, conflicting decisions, and late responses will be handled.

Most importantly, separate the review decision from the remediation. A reviewer's "revoke" decision is not proof that access was removed. The process should create a tracked action, assign an owner, set a deadline, and record completion. Keep the review record and the evidence of the resulting change linked.

## Move from Spreadsheets to User Access Review Automation

Automation can reduce manual preparation and chasing, but the goal is not simply to replace a spreadsheet with a screen. Effective user access reviews need a reliable data feed, a clear workflow, useful context for reviewers, and an evidence trail. Start by mapping how access data currently moves from each application into the review.

### Use flexible imports across many systems

Critical application data rarely comes from one clean source. Some systems offer connectors or APIs; others produce scheduled reports, database extracts, or administrator-generated files. An IAM platform should accommodate the organization's actual mix of systems rather than assuming every application has a modern integration.

When evaluating imports, ask whether the platform can handle common formats such as CSV and Excel, map source fields to a consistent data model, identify unique accounts, and flag records that fail validation. Find out how it handles changes between imports: Can it distinguish a new account from an existing one? Can it show when an entitlement has been added or removed? Can it retain the source and import date for each record?

For systems with multiple account types, confirm that the import can preserve those distinctions. A service account should not be silently assigned to an employee's manager merely because the file has a "manager" column. The workflow needs a meaningful owner, and missing ownership should appear as a data-quality issue to resolve—not disappear from the campaign.

Before automating a critical review, test the import against a known population. Reconcile record counts, compare a sample of accounts and entitlements to the source application, and investigate duplicates, missing fields, and unexpected changes. Automation makes repeatable errors faster, so validate the data before relying on the workflow.

### Design workflow assignment around real ownership

A review platform should make it possible to assign work by application, manager, entitlement owner, account type, or another useful rule. It should support delegated reviews and reassignment while preserving who made each decision and when. Reviewers should not need to search through an entire enterprise-wide list to find their responsibilities.

Good reviewer experience is a control consideration, not just a usability preference. Present enough context to support a decision: the account's owner, role, application, relevant activity, and any prior review outcome that is appropriate to show. Use plain-language instructions and clear options. A reviewer who cannot tell what an entitlement means is likely to approve it by default or send the question through an informal email thread.

Look for reminders, escalation rules, due dates, and dashboards that distinguish completed, overdue, disputed, and unassigned work. Confirm how the system handles reviewers who are unavailable, shared mailboxes, and administrator accounts that should not approve their own access. Avoid workflows that rely on a reply to an email as the only evidence of approval. The platform should capture the decision and its history directly.

## Choose Identity Governance Technology on Evidence, Not a Demo

Identity governance selection criteria should reflect the workflow you need to run—not only a feature list. Include application owners, IAM, information security, internal audit, and operational teams in the evaluation.

Ask each group what information it needs to make a decision and what evidence it will need afterward.

Evaluation area Questions to ask What to verify Data coverage Can the platform ingest our critical applications and different account types? Test real extracts, including service accounts, duplicate records, and missing owners. Workflow Can reviews be assigned by application, manager, owner, or account type? Run a sample campaign with reassignment, delegation, reminders, and escalation. Decision quality Can reviewers see enough context to make informed choices? Ask actual reviewers to complete a sample review and explain unclear items. Remediation How are revoke and modify decisions tracked to completion? Follow a sample decision from approval through verified access change. Evidence and reporting Where does the evidence live, and how is it retrieved later? Export a complete review history, including source data, decisions, timestamps, and remediation status. Administration Who can change campaigns, rules, or review results? Inspect role separation, administrative logs, and controls over configuration changes.

Ask vendors to demonstrate your workflow using representative data, not just a polished sample tenant. Include an application with a straightforward employee population and another with privileged, vendor, thesiliconreview or service accounts. Request proof of how exceptions, missing owners, late reviews, and remediation are handled.

Organizations may encounter providers with different backgrounds and offerings while assessing the market. For example, Member Driven Technologies (MDT) is relevant to conversations in the credit union technology ecosystem, while Security Compliance Corp (SCC) and Access Auditor may also come up during research into access review and compliance approaches. Treat any vendor discussion as a starting point for evaluation: confirm current capabilities, integrations, evidence handling, and fit against your specific requirements rather than assuming that a name alone establishes suitability.

## Make the Results Useful to IAM Controls and Audit

A completed campaign is not the outcome; a defensible access decision is. Retain enough information to show the population reviewed, the source and timing of the data, the assigned reviewers, their decisions, exceptions, and the status of resulting changes. Evidence should be retrievable from a defined system of record, not reconstructed from inboxes and personal folders when an audit begins.

When logs are available, use them to substantiate system activity rather than relying on screenshots. Screenshots can be useful for explaining a configuration, but they are often difficult to validate and may not show the full history. Prefer exportable audit logs or system records that identify the action, actor, target account, and timestamp. Document how those records are linked to review decisions.

Track operational measures that reveal where the process is breaking down. Useful measures include on-time completion, unassigned accounts, overdue decisions, revocations awaiting action, time to remediate, repeat exceptions, and records with no clear owner. A high completion rate can be misleading if reviewers approve everything without examining it, so pair completion statistics with sampling, exception analysis, and feedback from application owners.

## A Practical Implementation Sequence

1. **Inventory critical applications.** Record business owners, technical contacts, data sensitivity, account types, and access sources.
2. **Define review scope.** Specify which roles, groups, privileges, and identities are in scope, along with cadence and event-driven triggers.

3. **Map ownership.** Identify reviewers and delegates for employees, privileged accounts, vendors, and service accounts.
4. **Validate source data.** Reconcile imports to application records and resolve duplicates, missing owners, and unclear entitlements.
5. **Pilot the workflow.** Run one review with representative users and account types. Collect feedback on assignments, instructions, and context.
6. **Track remediation.** Turn revoke and modify decisions into owned, dated actions, and confirm completion in the source system.
7. **Retain and improve evidence.** Define where records live, test retrieval, review exceptions, and refine the process after each cycle.

## Make Every Review Traceable

Strong reviews for critical applications combine accurate data, accountable reviewers, practical workflows, and verified remediation. Spreadsheets can help establish the process, but automation becomes valuable when it reduces manual handling without weakening those controls. Flexible imports matter because access data comes from many systems. Clear workflow assignment matters because reviewers need relevant work and enough context to judge it. Evidence matters because an approval that cannot be traced is difficult to defend.

Design the review around the decisions the organization needs to make, then choose technology that can support those decisions end to end. When every account has an appropriate owner, every decision is recorded, and every required change is tracked to completion, user access reviews become a functioning IAM control—not just an annual exercise.