

## WHITE PAPER 01 / IDENTITY LIFECYCLE

# Building a Reliable Joiner, Mover and Leaver Process

A practical operating model for turning workforce changes into the right access changes, with clear ownership and verification.

AldentX Editorial | September 2026

## Executive summary

A person starting work, changing jobs or leaving the organisation creates a chain of access decisions. Each decision depends on accurate information, agreed responsibilities and a way to confirm that the intended change reached the application. This paper explains how to design that chain, handle exceptions and measure the result. It follows realistic workplace situations rather than assuming every person fits a standard employee record.

### What you will take away

- Define who supplies each lifecycle fact and when it takes effect.
- Treat a transfer as removal and addition, not just new access.
- Verify the resulting account state, including failed changes.

Written for hr operations, application owners and identity teams.

The worked scenarios are fictional. The checklists and examples are practical editorial guidance, not customer results or audited implementations.

# 1. Start with the working relationship

Identity governance and administration, often shortened to IGA, helps an organisation decide who should have access and manage that access over time. A joiner starts needing access, a mover changes responsibilities, and a leaver stops needing access. These events are easy to describe but can cross several systems and teams.

## Illustrative workplace case

Northbank Components is a fictional manufacturer. A planner transfers to procurement while a contractor starts a six-week maintenance assignment. The employee record comes from HR; the contractor record comes from a sponsor. Both need access, but their approval, expiry and exception arrangements differ.

Begin with the relationship that creates the business need. Employment status alone may not describe someone with two assignments or a contractor becoming an employee. Identify which record governs each relationship and how the organisation determines the access justified by it. Avoid using an email address as the only link between a person and their accounts.

Microsoft describes lifecycle workflows in terms of joiners, movers and leavers. The distinction is useful beyond any single product: the relevant change is the person's need for access, not just the arrival of a new account record. [Microsoft Learn: What are lifecycle workflows?](#)

# 2. Assign ownership to the information

List the information each workflow needs and who is accountable for its accuracy. HR may own an employee's start date and organisational assignment. A business sponsor may own a contractor's end date. The application owner decides which permissions support the job. The identity team maintains the connection between those facts and access changes.

| Information           | Accountable source          | If missing or inconsistent                                     |
|-----------------------|-----------------------------|----------------------------------------------------------------|
| Start or end date     | HR or authorised sponsor    | Hold scheduled changes for review; escalate urgent departures. |
| Business assignment   | Manager or workforce record | Request clarification before assigning a broad access role.    |
| Application ownership | Service owner register      | Route to a named fallback rather than an unmonitored queue.    |
| Account identity link | Identity integration owner  | Investigate matching conflicts before changing accounts.       |

Decide how late corrections are handled. A changed start date should not create a second identity. A cancelled departure should not blindly restore every historical permission. Keep a record of the correction, its authority and the resulting actions so support teams can explain what happened.

Record effective time as well as the date where it matters. Teams working across time zones need an agreed interpretation of when a departure or assignment change becomes active. Test that interpretation with the workforce-data owner before automating it.

### 3. Design the three paths separately

For a joiner, distinguish baseline access from permissions that need an explicit request. A standard collaboration account may follow an agreed rule, while access to supplier bank details may need a business owner's approval. Decide when accounts are created and when they become usable; those events do not have to be simultaneous.

For a mover, compare the old and new responsibilities. At Northbank, the planner may need purchase-order access but should not automatically retain planning exceptions granted for an earlier project. Ask which previous permissions should end and whether a short handover is justified. Give any overlap an owner and an end condition.

For a leaver, identify the accounts, access paths and dependent work that need attention. Disabling one directory account may not end application-local access or existing sessions everywhere. Transfer business ownership where needed, while keeping access-removal work separate from retention decisions about records and files.

- Joiner: confirm identity, start conditions, baseline access and additional approvals.
- Mover: remove obsolete access, assess conflicts and authorise any temporary overlap.
- Leaver: remove access, verify target-system state and assign unresolved exceptions.

## 4. Build failure handling into the workflow

A workflow needs more than a successful path. An application may be unavailable, an approver may be absent or a source record may arrive twice. Define who receives the failure, what can be retried safely and when a person must intervene. Do not mark the business outcome complete merely because an instruction was sent.

Test duplicate events and changes arriving out of order. A late update should not revive a departed person's access. Where a target system cannot be changed automatically, create an accountable manual step and require confirmation. Manual work is not necessarily a control failure; invisible manual work is much harder to govern.

| Scenario to test                   | Expected outcome                                                  |
|------------------------------------|-------------------------------------------------------------------|
| Duplicate joiner message           | One correctly linked identity and no duplicate entitlement grant. |
| Transfer with sensitive old access | Old access reviewed rather than silently retained.                |
| Unavailable target application     | Failed removal visible with an owner and escalation.              |
| Cancelled start                    | Pending access prevented or withdrawn through an approved action. |

Keep the exception record specific. Name the affected account and application, the intended state, the current known state and the next action. A general "workflow failed" message forces the next team to reconstruct the problem before it can help.

## 5. Use automation where the rule is understood

Automation is most useful when the input, decision and expected result are clear. Begin with a limited set of applications whose owners can validate the mapping. Compare the planned changes with a reviewed sample before broadening the population. Keep a controlled way to pause or correct a faulty rule.

IGAX's published lifecycle capabilities include HR-driven provisioning, role assignment and joiner, mover and leaver workflows. Its workflow designer and integration features support the configuration of these processes. Confirm target-system behaviour and exception handling during implementation. [IGAX platform capabilities](#).

Role suggestions can help identify plausible access for a job. They still need business interpretation. A peer group may contain inherited permissions that are no longer justified. Use the suggestion as a proposal, check sensitive access separately and establish who approves changes to the baseline.

At Northbank, the first deployment might cover ordinary procurement access while leaving bank-detail maintenance under separate approval. That boundary makes the workflow understandable and provides an opportunity to test the removal path before expanding the automation.

## 6. Measure completed outcomes

Measure whether access was ready when required and removed when required, with the definition and population stated. Separate source-data delays, approval delays and target-system failures. This helps the right team improve the process rather than attributing every delay to the identity platform.

For departures, compare the authorised effective time with verified removal for each in-scope access path. Record exceptions rather than hiding them in an average. For transfers, review whether old access was reconsidered and whether authorised overlaps expired. These checks reveal issues that a simple completed-workflow count can miss.

### Readiness checklist

Before widening the rollout, confirm named data owners, tested matching rules, joiner and mover removal paths, departure escalation, application-level verification and an operational owner for every exception.

Review the process after a reorganisation, a new HR integration or a material application change. The original mapping may no longer reflect how the organisation works. Preserve enough history to distinguish a new business requirement from an accidental return to an old permission set.

## References and further reading

Primary guidance used for the points cited in this paper. Examples, templates and recommended working practices are AldentX editorial guidance. Sources reviewed September 2026.

### [Microsoft Learn: What are lifecycle workflows?](https://learn.microsoft.com/en-us/entra/id-governance/what-are-lifecycle-workflows)

<https://learn.microsoft.com/en-us/entra/id-governance/what-are-lifecycle-workflows>

### [IGAX platform capabilities](https://www.aidentx.com/igax/platform)

<https://www.aidentx.com/igax/platform>

### Put the guidance into practice

Read related articles and explore IGAX platform capabilities at [www.aidentx.com/igax/resources](https://www.aidentx.com/igax/resources).