WHITE PAPER 05 / INTEGRATIONS AND ASSURANCE

Connecting Identity Governance to Operational Evidence

Build dependable integrations, handle provisioning failures and produce reporting that explains actual access outcomes.

AIdentX Editorial | September 2026

Executive summary

Identity governance depends on the information it receives and the actions its connections can perform. An approved request may be recorded correctly while the target application remains unchanged. A useful implementation closes that gap through explicit data ownership, tested integration behaviour and reconciliation. This paper shows how to connect lifecycle decisions, access execution and management reporting into a reviewable chain.

What you will take away

- Specify what each integration reads, changes and cannot do.
- Reconcile expected access with observed access.
- Report unresolved execution and evidence gaps alongside decisions.

Written for iam architects, application owners and assurance leads.

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

1. Map the chain from fact to outcome

A source system provides a fact, such as an employee changing departments. A policy or workflow determines the intended access. An integration sends the change to an application. The application's resulting state determines what access the person actually has. Reporting should preserve these separate stages.

> **Illustrative workplace case**
>
> Stonefield Services is a fictional business connecting its HR system, directory and service-management application. Transfers are recorded promptly in HR, but some permissions remain in the application because a group-removal operation fails. The dashboard must distinguish a processed transfer from a verified access change.

Draw the responsibility boundary for every stage. An identity team may own the workflow while an application team owns permission meaning and API access. A supplier may operate part of the target system. Name who can resolve a failure rather than assuming that the team receiving an alert can also fix it.

Record scope limitations early. If the integration reads accounts but cannot remove entitlements, the operating process needs a separate execution step. A connector name alone does not tell a business owner which outcomes are covered.

2. Define an integration contract

For each connected application, document identifiers, attributes, entitlement mappings and supported actions. Decide which system is authoritative for each field. A display name may change without changing the person; an account identifier must still be matched correctly.

Contract item	Question to resolve
Identity matching	How are source identities linked to target accounts?
Read coverage	Which users, groups, direct rights and statuses are visible?
Write coverage	Which grants, removals and updates are supported?
Timing	When should changes be observed, and how are delays detected?
Failure handling	Which failures can be retried, and who handles the others?

RFC 7644 defines the SCIM protocol for managing identity resources through HTTP operations. Protocol support does not, by itself, establish that a particular application exposes every permission or lifecycle action an organisation needs. IETF RFC 7644: SCIM Protocol.

Use a small set of real business operations as acceptance cases. Creating a test account is useful, but insufficient. Include a transfer, an entitlement removal, an account disablement and an unsuccessful operation. Verify the target state for each supported case.

3. Test failures as carefully as success

An integration can fail because of expired credentials, insufficient permissions, rate limits, target downtime or unexpected data. The handling should make the business impact visible without exposing secrets in error messages. A failed read may leave a stale inventory; a failed write may leave unwanted access active.

Retries need a defined purpose and limit. Repeating an account creation after a timeout can create duplicates if the original request succeeded but the response was lost. Establish how the integration determines the current target state before repeating consequential actions.

At Stonefield, the failed removal should remain assigned to an operational owner. The transfer workflow can show that its decision stage finished while the access outcome remains unresolved. This is more useful than a single successful status for the whole chain.

- Test unavailable targets and rejected credentials.
- Check duplicate messages and out-of-order changes.
- Confirm that retries do not create duplicate or unintended access.
- Verify how unsupported actions reach a manual owner.
- Record the evidence needed before an exception can close.

4. Reconcile intended and observed access

Reconciliation compares the access expected under the governance process with the access observed in the target system. Differences need interpretation. A local administrator may have granted access directly, a removal may be delayed or the mapping may not cover an indirect membership.

Do not automatically delete every unmatched account. It could be an operational account, a recently created identity or a matching error. Investigate ownership and purpose, then act through the authorised process. Equally, do not treat every unmatched record as harmless simply because it has existed for a long time.

Difference	Investigation
Expected grant absent	Was execution rejected, delayed or mapped incorrectly?
Unexpected entitlement present	Was it granted locally, inherited or retained after a change?
Account without a linked person	Is ownership known, and is the identity type correctly classified?
Status differs across systems	Which observation is current and which system owns the decision?

Set the reconciliation cadence according to the application and exposure. Distinguish the time a change was requested from the time it became visible in the data. A dashboard should not imply real-time certainty when the underlying source refreshes periodically.

5. Design reporting around decisions

A report should help its audience decide what needs attention. For an operations team, that may be failed removals and ageing exceptions. For a business owner, it may be unresolved certifications. For a sponsor, it may be important applications that remain outside integration coverage.

IGAX's published capabilities include connectors, workflow design, risk analytics and audit reporting. Use those capabilities to organise decisions and evidence, while documenting source coverage, refresh timing and supported actions for the actual deployment. IGAX platform capabilities.

Avoid presenting a risk score as a precise probability of compromise unless the method genuinely supports that interpretation. Explain the main contributing factors and what action the score should prompt. Keep missing information visible rather than allowing it to look like a low-risk result.

Separate decision, execution and verification metrics. A high percentage of approved requests says little about whether the resulting permissions were correct. A low count of open issues can also reflect incomplete coverage or closed duplicates rather than reduced exposure.

6. Assemble an evidence trail people can follow

For a material access change, retain the authorised trigger, applicable policy or approval, target action, result and verification. Record the time and responsible actor at each stage. Restrict access to the evidence according to its sensitivity and the organisation's retention requirements.

Prepare a sample trace before the first audit request. Choose a transfer with a complication, not only a clean new-account creation. Ask someone outside the implementation team to follow it from source event to final access state. Their questions will reveal missing context.

Operational acceptance test

For a selected access change, a reviewer can explain the intended outcome, locate the execution result, confirm the observed target state and identify any unresolved exception. The evidence does not depend on one engineer remembering the implementation.

Review the integration contract after application upgrades, permission-model changes or new identity populations. The work is complete only when the operating team can maintain the connection and explain failures. A working demonstration is the start of that assurance, not its permanent replacement.

References and further reading

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

IETF RFC 7644: SCIM Protocol

https://www.rfc-editor.org/info/rfc7644/

IGAX platform capabilities

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.