WHITE PAPER

Beyond Access.

Certifying what exists.

Why reviewing who has access is not enough, and how to certify the resource itself: its owner, its activity, its lifecycle, its privacy and its sharing.

EXECUTIVE SUMMARY

An access review checks the members.

Nobody checks the resource.

Access reviews answer one question well: who should keep getting in? They say nothing about the resource itself: whether it should still exist, whether someone answers for it, whether its data should be kept, or whether it is shared more widely than intended.

Resources outlive their reason for being. Created for a project, they stay open, retained or ownerless long afterwards, and an access review, which looks at members, never notices.

This paper describes resource certification: a set of policies that each ask a distinct question about a resource, and that call for an explicit decision from its owner, recorded with the same evidence as an access decision.

They stay open
Sharing granted for an assignment is never closed again.

They stay retained
Data whose usefulness has passed is kept by default.

They stay ownerless
The owner leaves; the resource carries on, answerable to no one.

One decision per policy
Keep, archive, restrict, reassign: never a mere "compliant".

CONTENTS

01 The blind spot of access reviews
02 One resource, several questions
03 Ownership comes first
04 Activity and lifecycle
05 Privacy and sharing
06 Decisions, not ticks
07 Where to start

01

The blind spot of access reviews

A document space created for an acquisition, a code repository from a discontinued product, a business application nobody has opened since a reorganisation: each of them can pass an access review with flying colours. The members are the right people; the access levels are reasonable. And yet the resource should not exist any more.

“An access review checks the members, not the resource.”

KEY IDEA

Resources are created easily and retired rarely. Each one carries data, sharing settings and an implicit owner. Over time, the estate fills with objects whose purpose is forgotten and whose risk is never reassessed.

Certifying the resource closes that gap. It asks whether the resource should exist and how it is governed, before asking who should get in.

DEFINITION

Resource certification: an explicit decision by the owner of a resource, on a given date, that the resource is still legitimate and governed as intended, policy by policy.

02

One resource, several questions

A resource is not certified on one dimension. Several policies apply, each with its own question, and they combine on a single resource depending on its nature and on what can be observed.

"Each policy asks a distinct question, and calls for its own decision."

KEY IDEA

POLICY	THE QUESTION IT ASKS
Ownership	Does the resource have an owner, and is it the right one?
Orphan	Has its owner left or become unknown: reassign or delete?
Inactivity	Has it been unused beyond a threshold: keep it or clean it up?
Data lifecycle	Is the data still needed: keep it, archive it or delete it?
Privacy	Does its visibility level match the intended level?
External sharing	Is sharing it outside the organisation still justified?
Internal oversharing	Is its internal audience too wide: confirm or restrict?
Custom	A generic certification policy, defined for a specific need.

03

Ownership comes first

Every other policy depends on this one. A resource without a responsible owner cannot be certified on anything else, because there is nobody whose decision would count.

Ownership is more than a field in an administration console. It is a commitment: a named person who has agreed to answer for the resource, and who is reachable. When that person changes role or leaves, the resource becomes orphaned, and the first decision to take is who will answer for it next.

Certifying ownership regularly is how an organisation keeps its estate answerable. It is also the precondition for every later decision on activity, retention or sharing.

"Without an owner, there is no one to decide."

KEY IDEA

Named
A person, not a team mailbox or a departed account.

Accepted
The owner has agreed to be one.

Reachable
Still in the organisation, still in a role that fits.

Reassigned
When they leave, the resource gets a new owner, not silence.

04

Activity and lifecycle

Inactive resources keep their access, their data and their sharing settings. They serve no one and expose something. An inactivity policy asks the owner, beyond a threshold set by policy, whether to keep the resource or clean it up.

Data lifecycle goes one step further. It asks whether the data the resource holds is still needed, and whether it should be kept, archived or deleted. Retention by default is the most common answer in practice, and it is rarely a decision anyone took.

Activity must be measured honestly. A date that reflects only a system's housekeeping is not a sign of use; activity means people or processes actually used the resource.

“What becomes of data should be a decision, not a default.”

KEY IDEA

DEFINITION

Inactivity threshold: the period without genuine use, set by policy, after which the owner is asked to decide whether the resource should remain.

05

Privacy and sharing

Three policies look at who can reach the resource, from the resource's point of view rather than the member's.

- **Privacy.** Does the visibility level of the resource match the level intended for its content?
- **External sharing.** Is sharing outside the organisation, opened for a partner or a project, still justified?
- **Internal oversharing.** Is the internal audience wider than it needs to be, for instance open to everyone when only a team needs it?

These questions differ from an access review: they are about the exposure of the resource as a whole, and the decision is to confirm or to restrict it, not to approve individual members.

"Sharing granted for an assignment is rarely closed again."

KEY IDEA

06

Decisions, not ticks

Resource certification produces explicit decisions. Each policy has its own outcome: keep or clean up, keep or archive or delete, confirm or restrict, reassign. A single "compliant" checkbox would erase the very information that makes the decision useful.

What must change is tracked until an observation confirms it. A remediation is closed only when the next collection shows the resource in the state the owner decided.

The decisions carry the same evidence as access decisions: author, date, justification and observed state, signed and sealed. The resource and those who access it are certified on the same foundation, by the same owners.

“Keep, archive, restrict, reassign: never a mere "compliant".”

KEY IDEA

07

Where to start

Resource certification can begin small and widen as observation improves.

1 **Inventory the resources** of the platforms that hold your most sensitive data.

2 **Certify ownership first,** and resolve orphaned resources before anything else.

3 **Add inactivity and lifecycle** with thresholds your owners can accept.

4 **Review privacy and sharing** where exposure is highest.

5 **Certify access on the same foundation,** with the same owners and the same evidence.

“Start with ownership. Everything else depends on it.”

KEY IDEA

REVYCORE

Resources someone answers for, and the proof that they did.

Human decisions. Verifiable evidence.

Request a demonstration in your context: your solutions, your scopes, your agents.

revycore.com

This paper describes an approach and the corresponding capabilities of REVYCORE for information purposes; it is not legal advice. The policies that apply depend on the nature of each resource and on what each solution allows to be observed. © 2026 REVYCORE SAS.