REVYCORE

WHITE PAPER

Continuous Certification.

Beyond the Point-in-Time Access Review

REVYCORE RESEARCH

DECEMBER 2026

EXECUTIVE SUMMARY

A certification is a fact about the past. Its validity is a question about today.

Access reviews were designed for a slower world. Once or twice a year, owners confirm who should have access to what, and the result is filed as evidence. The day after, the estate has already moved.

People change roles, workspaces are opened to outsiders, owners leave, AI agents receive new tools. The certification still describes the system as it was. Between two campaigns, nothing tells anyone that it no longer holds.

This paper describes continuous certification: an approach that keeps each human decision with its conditions and its term, reassesses its validity as new observations arrive, and calls on the right owner only when something significant has changed.

01 Proving a decision is not enough
The question is no longer whether a review took place, but whether what was certified still holds.

02 Six states, never one indicator
Still valid, re-attestation needed, expired, not verifiable, not comparable, in remediation.

03 Only what changed goes back
A targeted obligation reaches the owner concerned, without relaunching a whole campaign.

CONTENTS

01 The half-life of a certification
02 What changes between two campaigns
03 Six states, never blended
04 One cycle, six capabilities
05 Derived validity: sets and their components
06 What continuous certification does not claim
07 Campaigns and continuity, together
08 Where to start

01

The half-life of a certification

A human certification produces a historical attestation: on a given date, a named person decided that a given access, or a given resource, was legitimate. That fact remains true forever. Its relevance does not.

Every certification starts to age the moment it is signed. The longer the interval between two reviews, the larger the share of the estate whose certified state no longer matches reality, and the less the last campaign says about the risk carried today.

Shortening the cycle does not solve the problem. Reviewing everything more often multiplies the work, tires the reviewers and turns certification into a formality. What is needed is not more reviews, but a way to know which certifications still hold.

> **March's certification still describes March's system.**

02

What changes between two campaigns

The changes that invalidate a certification are ordinary. None of them is an incident; together, they are the drift that periodic reviews never see.

- **A change of role.** The person keeps the access of their previous function, which nobody revokes because nobody is asked.
- **A workspace opened to outsiders.** External sharing is enabled on a resource that was certified as internal.
- **An owner who leaves.** The resource has nobody left to answer for it, and its certification has no one to renew it.
- **A group whose composition changes.** The access was certified for twelve people; it now covers forty.
- **An AI agent with a new tool.** Its purpose was attested; its capabilities have since been extended.
- **An identity that changes.** A service or execution identity is replaced or shared, and actions can no longer be attributed.

03

Six states, never blended

"Compliant" and "non-compliant" erase exactly what an auditor wants to know. A certification can stop holding for very different reasons, and each one calls for a different response. Continuous certification names each situation.

STATE	WHAT IT MEANS, AND WHAT FOLLOWS
Still valid	The conditions of the decision are still met at the last observation, and the term has not been reached. No action: the attestation is maintained.
Re-attestation needed	A significant change has been detected: permission, composition, owner, execution identity, audience. A targeted obligation is sent to the decision-maker concerned.
Expired	The maximum term has passed. An attestation cannot stay valid indefinitely, even without change. A new decision is required.
Not verifiable	Collection is insufficient or interrupted. Nothing shows that the conditions hold, or that they no longer do. Observation must be restored; nothing is presumed.
Not comparable	The observation exists but can no longer be reconciled with the reference state, after a change of model, connector or scope. A new baseline is built.
Refused, in remediation	The owner refused. The correction is tracked until a later observation confirms it, and is closed only once verified.

04

One cycle, six capabilities

Continuous certification is not a monitoring dashboard. It is a cycle that links observation to human decision, and decision to evidence.

01

Observe

Information from connected solutions is collected at its own pace, reconciled with identities and owners, dated and kept.

02

Maintain

As long as an attestation's conditions are still met, it is maintained. Nobody is asked to restate what has not changed.

03

Detect

Significant changes and expiries are identified. A change to one component lowers the validity of the set it belongs to, and only that set.

04

Re-attest

Targeted obligations reach the right decision-maker, organised in continuous cohorts. The owner sees what changed, not a whole list to revalidate.

05

Remediate

Refusals, time-limited exceptions and corrective actions are tracked. A remediation is closed only when the next observation confirms it.

06

Prove

Decisions, authorities, observations and sealed evidence are reported as of a given date. What was certified on 30 May reads as it was on 30 May.

05

Derived validity: sets and their components

Certifications are rarely isolated. A business application, a data platform or a technology scope is made of components, each with its own owner and its own access. When one of them changes, the question is not only whether that component is still compliant, but whether the certification of the whole still holds.

Continuous certification answers with derived validity. A significant change to one component lowers the validity of the set it belongs to, without touching the others. The owner of the set is asked about that change, and only that change; the rest of the estate is left undisturbed.

History is never rewritten. When a new decision is taken, the former attestation stays readable as it was. For an auditor, the result is a continuous series of dated evidence rather than two snapshots a year apart.

> **Only what changed goes back to its owner.**

06

What continuous certification does not claim

Credibility depends on stating the limits as clearly as the capabilities. Four boundaries frame the approach.

FOUR BOUNDARIES

01

No universal real time

Monitoring follows the pace of the collections and signals available for each solution. Freshness is displayed, never assumed.

02

No automatic decision

Automatic assessment never replaces a human decision. It triggers it, targets it and keeps it.

03

No presumption

Insufficient collection never means an entitlement is compliant, nor that an attestation is currently verifiable.

04

No eternal validity

Every attestation carries a maximum term. Formal campaigns remain available for regulatory obligations.

07

Campaigns and continuity, together

Continuous certification does not abolish campaigns. Regulations such as DORA set a cadence for access reviews, and auditors expect to see it kept. Formal campaigns remain the backbone of that obligation.

What changes is what happens between them. Instead of six or twelve months of silence, the estate is observed, significant changes are routed to their owners, and each decision joins the same chain of evidence as the campaign that preceded it.

The next campaign then starts from a known state. Owners review what genuinely needs a decision, not hundreds of lines that have not moved, and the auditor sees an unbroken line from one review to the next.

08

Where to start

Moving from periodic to continuous certification is a progression, not a switch.

1. **Certify with conditions and a term.** Each decision should record what it relied on and how long it is meant to last.
2. **Name an owner for every resource and every set.** Derived validity needs someone to answer for the whole as well as for its parts.
3. **Connect the sources that matter first.** Start with the systems that support critical functions, where drift costs the most.
4. **Define what counts as significant.** Permission, composition, owner, identity, audience: decide which changes call for a new decision.
5. **Keep campaigns, and fill the gap between them,** so that every decision, periodic or targeted, joins the same sealed evidence.

REVYCORE

Certified yesterday.
Provable today.

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.
Continuous assurance is included in the REVYCORE Unlimited edition. © 2026 REVYCORE SAS.