REVYCORE

WHITE PAPER

Demonstrable Compliance.

DORA & Access Governance

REVYCORE RESEARCH

DECEMBER 2026

EXECUTIVE SUMMARY

Reviewing access is required. Proving it is what counts.

Since 17 January 2025, financial entities in scope of the Digital Operational Resilience Act (DORA) must review the access rights to their ICT systems at least once a year, and at least every six months for systems supporting critical or important functions.

Most organisations already run access reviews. Few can demonstrate them. On audit day, a spreadsheet export and a trail of approval emails describe an intention; they do not prove a decision.

This paper sets out what the texts actually require, what an auditor or supervisor will ask, why traditional reviews struggle to answer, and the principles of an access governance that produces its own evidence: named owners, frozen scopes, verified withdrawals, sealed attestations, and certifications that remain valid as the estate changes.

01 Once a year, every six months
DORA sets the pace: annual for ICT systems, six-monthly for those supporting critical or important functions.

02 A review is not evidence
The auditor will ask who decided, on what scope, how often, and whether refused rights actually disappeared.

03 Evidence is produced as you go
Decisions made by named owners, then signed and sealed, are ready for the auditor without being rebuilt.

CONTENTS

01 From governance performed to governance demonstrated
02 What the texts actually require
03 What the auditor will ask
04 Why traditional reviews fall short
05 Six principles of demonstrable access governance
06 From requirement to evidence
07 Between two campaigns
08 Where to start

01

From governance performed to governance demonstrated

For years, access reviews have been judged on a simple criterion: did the campaign take place? A spreadsheet was sent to managers, most lines came back approved, and the exercise was filed until the following year.

DORA changes the question. Financial supervisors no longer ask whether a review exists; they ask whether the institution can show, for any system and any date, who held which access, who decided to keep it, and on what basis. Governance has to be **demonstrated**, not merely performed.

This shift has a practical consequence. Evidence can no longer be assembled the night before the audit from scattered exports. It has to be produced at the moment of each decision, attached to it, and preserved in a form that a third party can verify.

> **Governance is an intention. Evidence is a fact.**

02

What the texts actually require

Regulation (EU) 2022/2554 has applied since 17 January 2025 (Article 64). Its Article 9 sets the principle; Commission Delegated Regulation (EU) 2024/1774 details access control in Articles 20 and 21, and a simplified framework in Article 33.

REFERENCE	REQUIREMENT
DORA, Art. 9(4)(c)	Limit physical or logical access to what is required for legitimate and approved functions and activities only, and ensure a sound administration of access rights.
RTS, Art. 21(a)	Assign access rights on need-to-know, need-to-use and least-privilege principles, including for remote and emergency access.
RTS, Art. 21(e)(i)	Assign roles and responsibilities for granting, reviewing and revoking access rights.
RTS, Art. 21(e)(ii)	Assign privileged, emergency and administrator access on a need-to-use or ad-hoc basis only.
RTS, Art. 21(e)(iii)	Withdraw access rights without undue delay upon termination of employment or when the access is no longer necessary.
RTS, Art. 21(e)(iv)	Update access rights at least once a year for ICT systems, and at least every six months for those supporting critical or important functions.
RTS, Art. 20	Extend the policy to the staff of ICT third-party service providers who access the entity's assets.
RTS, Art. 33(e)	Entities under the simplified framework review access rights periodically and withdraw them when no longer required.

Two points deserve attention. First, the frequency is written in black and white: a cadence missed on a critical system is a finding, not a matter of interpretation. Second, the text speaks of **roles and responsibilities**: the review must be carried out by people whose authority is defined, not by whoever happens to receive the spreadsheet.

DORA is not alone. NIS2, ISO/IEC 27001 and SOC 2 all expect access rights to be reviewed at regular intervals by accountable people. An approach built for DORA serves them all.

03

What the auditor will ask

A review took place. It still has to be demonstrated. Whatever the framework, the auditor's questions reduce to four.

THE FOUR QUESTIONS

01

Who decided?

A named person, with the authority they held at the time of the decision.

02

On what scope?

The systems and rights reviewed, frozen at launch, and the justified exclusions.

03

How often?

Dated occurrences proving that each deadline was met, system by system.

04

And the withdrawal?

Evidence that every refused right actually disappeared from the system.

04

Why traditional reviews fall short

Traditional campaigns were designed to be carried out, not to be proven. Their weaknesses show precisely where the auditor looks.

- **The wrong reviewer.** The line manager approves access to systems they do not know. The person who understands the resource, its owner, is never asked.
- **Rubber-stamping.** Hundreds of lines, one deadline, an "approve all" button. The decision exists on paper, not in substance.
- **A moving scope.** The extract changes during the campaign; nobody can say afterwards exactly what was reviewed.
- **Unverified withdrawals.** A right is refused, a ticket is opened, and the trail stops there. Whether the access actually disappeared is never confirmed.
- **Evidence rebuilt after the fact.** Exports, emails and screenshots are gathered before the audit. They describe a story; they can be edited, and they prove little.
- **A frozen snapshot.** The certification describes the estate on the day of the review. The next day, people move, resources open up, AI agents gain permissions, and nothing signals it.

05

Six principles of demonstrable access governance

An access governance that can be demonstrated rests on a few principles. None of them is a technology choice; each is a property the evidence must have.

01

Named owners decide

The person who knows the resource takes the decision. Reviewers are designated by rule, with a fallback and escalation, never improvised.

02

The scope is frozen

What is reviewed is fixed at launch, with any exclusions justified. The evidence describes exactly that scope.

03

Every decision is justified

A decision carries its reason, its date and the policy that called for it. It is not a tick in a column.

04

Withdrawals are verified

A refusal opens a correction that stays open until a later collection confirms the right has gone. An exception is temporary, with a reason and a deadline.

05

Evidence is sealed

Closure is signed by a named person, then sealed with decisions, reviewers, timestamps and scope, so it can be verified independently.

06

Certification stays current

When the estate changes significantly, the validity of what was certified is reassessed, and only what changed goes back to its owner.

06

From requirement to evidence

REVYCORE was built on these principles. It certifies resources, their access, technology scopes and AI agents against your policies; owners decide; the evidence remains. The table below maps each DORA expectation to what the platform produces.

DORA EXPECTATION	WHAT REVYCORE PRODUCES
Annual or six-monthly review	Periodic campaigns whose cycle is set in months: twelve for the estate, six for systems supporting critical or important functions. Each occurrence is dated and forms a series.
Roles and responsibilities	Reviewers designated by rule: owners, manager, a dedicated team or an attribute, with fallback and escalation. The administrator organises the review; they never decide in the owners' place.
Least privilege	Access policies that ask the right question: membership, access level, privileged access, guests, role definition.
Withdrawal without undue delay	Each refusal opens a correction, tracked until a later collection confirms the right has gone.
Sound administration of access rights	Closure signed by a named person, then sealed with the decisions, reviewers, timestamps and frozen scope. The package is verified offline.
Supervisory access	A read-only Auditor role, bounded by an end date: the auditor consults, verifies and exports, without running a campaign or deciding.
Third-party providers	Provider and guest accounts reviewed like the others, with a dedicated policy for guest access.

REVYCORE adds to your identity and access tools without replacing them. They grant rights and authenticate; REVYCORE runs the review, records the decisions and provides the evidence. Where an identity governance suite is already in place, the two are complementary.

07

Between two campaigns

A six-month cycle leaves six months during which the estate keeps changing. An owner leaves, a site is shared externally, an AI agent receives a new tool. The last certification still describes the previous state of the system.

Continuous certification closes that gap. Each decision stays attached to what it certified. When a significant change occurs, the validity of the certification is reassessed and the right decision-maker is asked, without waiting for the next campaign and without relaunching one. What was certified on a given date still reads as it was on that date.

For the auditor, the result is a continuous series of evidence rather than two snapshots a year apart. For the organisation, risk is addressed when it appears, not when the calendar says so.

> **Risk doesn't wait for your next campaign.**

08

Where to start

Demonstrable compliance does not require a multi-year programme. Five steps put an organisation on the right path.

1. **Map your critical or important functions** and the ICT systems that support them. They set the six-month cadence.
2. **Name an owner for each system and resource.** Without an owner, there is no one to decide and no one accountable.
3. **Define your policies** for access and for resources: what must be reviewed, by whom, and how often.
4. **Run a first campaign with a frozen scope** and require a justification for every decision.
5. **Seal the evidence and give your auditor read access,** then let continuous certification keep it current between campaigns.

REVYCORE

From Governance to Evidence.

Human decisions. Verifiable evidence.

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

revycore.com

This paper summarises public texts for information purposes; it is not legal advice. Overall DORA compliance belongs to each entity's ICT risk management framework. References: Regulation (EU) 2022/2554; Commission Delegated Regulation (EU) 2024/1774. © 2026 REVYCORE SAS.