WHITE PAPER

NIS2 & Access Governance.

Review at planned intervals. Document the result.

What the directive and its implementing regulation require of access reviews, and how to produce the evidence an auditor will ask for.

EXECUTIVE SUMMARY

NIS2 makes access control a measure. Its regulation makes it a record.

The NIS2 Directive lists access control policies among the minimum cybersecurity risk-management measures. For the digital service providers it covers, Implementing Regulation (EU) 2024/2690 spells out what that means: rights assigned on need-to-know, access authorised by the relevant persons, and a review of access rights at planned intervals, with documented results.

The text sets no frequency. It asks the entity to define its own intervals and to keep to them, which turns the review into a commitment that can be checked.

This paper walks through the relevant provisions, the questions an auditor will derive from them, and the properties a review must have to answer those questions with evidence rather than with assurances.

A minimum measure
Access control policies are named in Article 21(2)(i) of the Directive.

Planned intervals
Point 11.2.3: review at intervals you define, and keep.

Documented results
The review and the changes it decided must be recorded.

Privileged accounts too
Point 11.3.3 applies the same discipline to administrator accounts.

CONTENTS

01 From directive to regulation
02 What the text actually says
03 The questions an auditor will ask
04 The relevant persons
05 Third parties and privileged accounts
06 Documenting the result
07 Where to start

01

From directive to regulation

Directive (EU) 2022/2555, known as NIS2, sets the cybersecurity risk-management measures that essential and important entities must take. Article 21(2) lists them; point (i) covers human resources security, access control policies and asset management.

For a defined group of digital service providers, Implementing Regulation (EU) 2024/2690 details those measures in technical terms. Among others, it covers DNS and cloud computing service providers, data centre service providers, managed service and managed security service providers, online marketplaces and trust service providers. For other entities, the national transposition measures apply.

“The directive names the measure. The regulation describes the evidence.”

KEY IDEA

The difference matters. The directive says that access must be controlled; the regulation says how that control is to be shown.

DEFINITION

Planned intervals: a review frequency decided in advance by the entity, recorded, and kept, as opposed to a review carried out when someone remembers.

02

What the text actually says

Four points of the implementing regulation's annex bear directly on access reviews.

"No figure for the frequency, but no ambiguity about the record."

KEY IDEA

REFERENCE	REQUIREMENT
Directive, Art. 21(2)(i)	Human resources security, access control policies and asset management are among the minimum measures.
Regulation, point 11.2.2	Assign and revoke rights on need-to-know, least privilege and separation of duties; have access authorised by the relevant persons; limit third-party access in scope and duration.
Point 11.2.2 (f)	Apply logging to the management of access rights.
Point 11.2.3	Review access rights at planned intervals and document the results of the review, including the necessary changes.
Point 11.3.3	The same requirement for privileged accounts and system administration accounts.

Quotations and references are summarised from the published texts; the entity remains responsible for its own reading of its obligations.

03

The questions an auditor will ask

Each requirement translates into a question that can only be answered with a record. Assurances, procedures and screenshots do not answer them.

“A review took place. It still has to be documented.”

KEY IDEA

Who authorised it?

The relevant persons, by name, not an administrator acting for everyone.

At what intervals?

A frequency set in advance, and dated occurrences proving it was kept.

With what results?

The documented review, including the changes it decided.

And third parties?

External access limited in scope and duration, and reviewed as such.

04

The relevant persons

Point 11.2.2 asks that access be authorised by the relevant persons. In practice, the person best placed to say whether an access is still needed is the owner of the resource or the manager of the person, not the IT administrator who processes requests.

A review that routes every line to a central team produces decisions without authority. A review that designates reviewers by rule, with a fallback and an escalation when someone is absent, produces decisions that can be attributed and defended.

The separation of duties named in the same point applies to the review itself: the person who grants an access should not be the only one who confirms it.

“The administrator organises the review. The owner decides.”

KEY IDEA

05

Third parties and privileged accounts

Two populations call for particular care. Third-party access must be limited in scope and duration; guest accounts and provider accounts should therefore be certified with a policy of their own, and any exception should carry a reason and an end date.

Privileged and administration accounts fall under point 11.3.3, which repeats the review requirement. They are usually few, and each one matters; reviewing them at their own, shorter interval is a reasonable reading of the text.

“The accounts that carry the most risk deserve their own rhythm.”

KEY IDEA

- **Guests and providers.** A dedicated policy, a named sponsor, a scope and an end date.
- **Administrators.** A separate review, at its own pace, with decisions that are never self-approved.
- **Exceptions.** Temporary by construction: a reason, an owner and a deadline.

06

Documenting the result

Point 11.2.3 asks for the results of the review to be documented, including the necessary changes. A completed spreadsheet does not meet that bar on its own: it does not show who decided each line, under which authority, on which frozen scope, or whether the refused rights actually disappeared.

A documented result has four properties: each decision is attributed to a named person and dated; the scope reviewed is fixed at launch; refusals are tracked until a later observation confirms the change; and the closure is signed, then sealed, so that the record can be verified later without trusting whoever produced it.

Logging, required by point 11.2.2 (f), completes the picture: every decision is chained into an audit trail that can be streamed to the security operations centre.

"Evidence is produced at the moment of the decision, not before the audit."

KEY IDEA

DEFINITION

Verified withdrawal: a refused access is considered removed only once a later collection confirms that it has gone from the system.

07

Where to start

NIS2 leaves the frequency to the entity. That freedom is also a commitment: once set, the intervals become the benchmark against which the review is judged.

“Choose your intervals, then keep them.”

KEY IDEA

1 **Map the systems in scope** and identify the privileged and third-party accounts among them.

2 **Set your planned intervals** per scope, and record the decision.

3 **Designate the relevant persons** by rule, with a fallback and an escalation.

4 **Run each review on a frozen scope** and require a justification for every decision.

5 **Sign, seal and keep the results,** and give your auditor read access to verify them.

REVYCORE

Review at planned intervals.
Prove every one of them.

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 NIS2 compliance belongs to each entity's cybersecurity risk-management framework. References: Directive (EU) 2022/2555; Commission Implementing Regulation (EU) 2024/2690. © 2026 REVYCORE SAS.