REVYCORE

WHITE PAPER

The Auditor's Questions.

And the evidence that answers them.

A method for preparing access reviews from the auditor's side of the table: the questions every framework leads to, and what a convincing answer looks like.

KNOWLEDGE CENTER

DECEMBER 2026

EXECUTIVE SUMMARY

The auditor does not read the policy.

They ask for the evidence.

DORA, NIS2, ISO 27001 and SOC 2 use different words, but their access review requirements lead the auditor to the same handful of questions: did the review happen, who decided, on what population, how often, and what became of the rights that were refused.

Most audit pain comes from answering those questions after the fact, by assembling exports and emails into a narrative. The same questions are far easier to answer when the review is designed around them from the start.

This paper lists the questions, explains what the auditor is really testing behind each one, and describes the evidence that answers it without discussion.

Same questions
Four frameworks, one set of questions about access reviews.

Tested, not read
Policies describe intent; auditors test occurrences and samples.

Every occurrence
Over a period, one good review does not cover a missing one.

Answered by design
Evidence produced at decision time needs no reconstruction.

CONTENTS

01 Why the questions converge
02 Did the review take place?
03 Who decided?
04 On what population?
05 What became of the refusals?
06 Privileges, third parties, and integrity
07 Preparing from the auditor's side

CHAPTER 01

Why the questions converge

Different frameworks, the same handful of questions.

Each framework frames access reviews in its own terms. DORA's technical standards set an annual or six-monthly pace; NIS2's implementing regulation asks for reviews at planned intervals with documented results; ISO 27001 places the review of access rights in control A.5.18; the SOC 2 criteria expect access to be reviewed periodically and removed when no longer authorised.

Behind the vocabulary, the auditor's job is the same: to obtain reasonable assurance that access is controlled, and that the control operates as described. That leads to the same questions, whatever the framework.

Preparing for one audit therefore prepares for the others, provided the evidence is built around the questions rather than around a particular checklist.

Operating effectiveness DEFINITION

the demonstration that a control did not merely exist on paper, but actually ran as described, every time it was supposed to.

CHAPTER 02

Did the review take place?

One good review does not cover a missing one.

The first question sounds trivial and is often the hardest. The auditor wants each occurrence the policy promised, dated, for each scope. In a SOC 2 Type II, every review planned over the observation period must be evidenced; a single gap is an exception in the report.

The answer is a series, not a document: dated occurrences, per scope, at the frequency written in the policy. A cycle set in months and a calendar that the tool keeps by itself make the series hard to break and easy to show.

What is tested
The frequency in the policy, against dated occurrences.

Typical gap
A quarter skipped during a reorganisation, discovered at audit.

Convincing answer
A series of campaigns, one per period and per scope, each dated.

Where it fails
Reviews run by hand, with dates reconstructed from emails.

CHAPTER 03

Who decided?

The asset owner, not the team that administers it.

Auditors look for decisions taken by people who know the asset and have the authority to decide. A review in which an administrator approves hundreds of lines on behalf of everyone fails this test, however complete it looks.

The answer is a designated reviewer per line, chosen by rule (owner, manager, a dedicated team or an attribute), with a fallback and an escalation when someone is absent, and a justification attached to each decision. The administrator organises the review; they do not decide in the owners' place.

Authority is judged at the time of the decision. Evidence should therefore record not only who decided, but under which role and assignment they were entitled to.

CHAPTER 04

On what population?

A complete scope, frozen at launch.

The auditor will ask whether the review covered everything it should have. A population extracted by hand, edited during the campaign, or silently filtered, cannot be shown to be complete.

The answer is a scope computed from the connected systems and frozen when the campaign is launched. Exclusions are allowed, but they are justified and visible. The auditor can then pick a sample from a population they can trust.

- **Computed.** From the systems themselves, not from a spreadsheet.
- **Frozen.** Fixed at launch, so that the evidence describes exactly what was reviewed.
- **Justified exclusions.** Anything left out is named, with its reason.
- **Sample ready.** Decisions, reviewers and timestamps sealed with the campaign.

CHAPTER 05

What became of the refusals?

A refused right is removed only when a later observation confirms it.

A review that refuses access but never removes it is worse than no review: it documents a known risk left in place. Auditors increasingly ask for evidence that every refused right actually disappeared.

The answer is a correction opened for each refusal and tracked until a later collection confirms that the right has gone. Exceptions are possible, but they stay temporary, with a reason, an owner and a deadline.

> **Verified withdrawal** DEFINITION
> the closure of a refusal only once a subsequent observation shows the right is no longer present in the system.

CHAPTER 06

Privileges, third parties, and integrity

The riskiest accounts and the record itself are tested too.

Three further questions recur. Privileged accounts are expected to be reviewed on their own, often more frequently. Third-party and guest access must be limited in scope and duration. And the record of the review must be shown not to have been altered since.

QUESTION	CONVINCING ANSWER
Privileged access?	A policy dedicated to privileged access, reviewed at its own pace, never self-approved.
Third parties and guests?	A dedicated policy, a named sponsor, a scope and an end date for every exception.
Unaltered since?	Closure signed by a named person, then sealed; the package verified offline, without an account.
Valid on a given date?	The state of certifications as of the date requested, read as it was, not as it has become.

CHAPTER 07

Preparing from the auditor's side

Design the review around the questions, not the checklist.

The simplest preparation is to give the auditor a direct, read-only view of the evidence: an Auditor role bounded by an end date, from which they consult, verify and export without running a campaign or deciding anything.

01 **Write the frequency in the policy,** per scope, and let the tool keep the calendar.

02 **Designate reviewers by rule,** with justification required for every decision.

03 **Freeze the population at launch** and name every exclusion.

04 **Track every refusal** until a later observation confirms the removal.

05 **Seal the result and open a read-only view** for the auditor, bounded in time.

REVYCORE

Every question,
answered by evidence.

Human decisions. Verifiable evidence.

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

revycore.com

This paper summarises public frameworks for information purposes; it is neither legal advice nor an audit opinion. ISO/IEC 27001 is published by ISO and the Trust Services Criteria by the AICPA; their content is summarised, not quoted. © 2026 REVYCORE SAS.