REVYCORE

WHITE PAPER

Privileged Access Reviews.

Few accounts. Every one of them matters.

Why every framework singles out privileged accounts, and how to review them on their own terms, at their own pace, without self-approval.

KNOWLEDGE CENTER

DECEMBER 2026

EXECUTIVE SUMMARY

The accounts that can change everything

deserve their own review.

Administrator, emergency and system accounts are few, but each one can change configurations, read any data or disable controls. That is why DORA, NIS2, ISO 27001 and SOC 2 all treat privileged access as a category of its own.

Reviewing privileges inside a general access campaign dilutes them among thousands of ordinary lines, often in front of reviewers who hold the same privileges.

This paper explains what the frameworks ask, why privileges need a dedicated review, and how to make that review rigorous: separate policy, own rhythm, independent reviewers and verified removal.

A category of its own
Named specifically by all four frameworks.

Its own rhythm
Often more frequent than ordinary reviews.

No self-approval
A privilege is never confirmed by its holder.

Need-to-use
Granted for a purpose, removed when it ends.

CONTENTS

01 Why privileges are different
02 What the frameworks ask
03 A review of their own
04 Who reviews the reviewers?
05 Emergency access
06 Where to start

CHAPTER 01

Why privileges are different

Few accounts. Every one of them matters.

An ordinary account reaches what its owner needs. A privileged account reaches what everyone needs: it can create accounts, change permissions, read data across the estate, or turn off the controls that would detect misuse.

Privileges also accumulate silently. Emergency access granted during an incident stays; a former administrator keeps their rights after moving to another team; a service account receives broad permissions to make an integration work.

Privileged access DEFINITION

rights that allow changing the configuration or security of a system, or reaching data beyond an individual's own need, including administrator, emergency and system accounts.

CHAPTER 02

What the frameworks ask

Four frameworks, one consistent expectation.

Each framework addresses privileged access explicitly. The references below are summarised.

FRAMEWORK	EXPECTATION (SUMMARISED)
DORA, RTS Art. 21(e)(ii)	Privileged, emergency and administrator access assigned on a need-to-use or ad-hoc basis only.
NIS2, Reg. point 11.3.3	Review requirements applied to privileged accounts and system administration accounts.
ISO 27001, A.8.2	The allocation and use of privileged access rights restricted and managed.
SOC 2, CC6.3	Access granted on roles and responsibilities, considering least privilege and segregation of duties.

CHAPTER 03

A review of their own

Diluted among thousands of lines, privileges go unseen.

A dedicated privileged access policy separates these accounts from ordinary campaigns. It can run more often, involve different reviewers, and ask sharper questions: what is this privilege for, is that purpose still current, and could a narrower right serve it?

- **Separate policy.** Privileges reviewed on their own, never mixed with ordinary access.
- **Own rhythm.** A shorter interval where the risk justifies it.
- **Purpose stated.** Each privilege tied to a reason that can be checked.
- **Narrower alternative.** The question of whether less would do is always asked.

CHAPTER 04

Who reviews the reviewers?

A privilege is never confirmed by its holder.

Privileged access creates a particular trap: the people best placed to understand administrator rights are often administrators themselves. A review in which they confirm their own privileges, or each other's without independence, proves little.

The rule is simple to state: the holder of a privilege never decides on it, and the review should be taken by someone with authority over its purpose, such as the owner of the system or the manager of the holder.

Independent
Never the holder of the privilege.

Accountable
The system owner or the holder's manager.

Justified
Each decision with its reason.

Escalated
An absent reviewer is replaced by rule, not by habit.

CHAPTER 05

Emergency access

Granted for an incident. Removed after it.

Emergency, or break-glass, access is legitimate: incidents require rights that ordinary operations do not. It becomes a risk when it outlives the incident.

Treating emergency access as a time-limited exception, with a reason, an owner and an end date, keeps it legitimate. When the date passes, the access is removed, and the removal is confirmed by a later observation.

> **Need-to-use** DEFINITION
> a privilege granted only for a specific need and removed as soon as that need ends.

CHAPTER 06

Where to start

Find every privilege before you review any.

Privileged access reviews start with a complete list, which is often the hardest part.

01 **Inventory privileged accounts** including emergency and service accounts.

02 **Tie each privilege to a purpose** and an owner who answers for it.

03 **Review them in a dedicated policy,** at their own, shorter interval.

04 **Exclude self-approval** and escalate by rule.

05 **Time-limit emergency access** and verify every removal.

REVYCORE

Every privilege,
a purpose and a decision.

Human decisions. Verifiable evidence.

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

revycore.com

Framework references are summarised for information purposes; ISO/IEC 27001 is published by ISO and the Trust Services Criteria by the AICPA. This paper is neither legal advice nor an audit opinion. © 2026 REVYCORE SAS.