REVYCORE

WHITE PAPER

Segregation of Duties.

In the access you review, and in the review itself.

How separation of duties applies twice in access certification: to the combinations of rights being reviewed, and to the people who run and decide the review.

KNOWLEDGE CENTER

DECEMBER 2026

EXECUTIVE SUMMARY

Segregation of duties applies twice:

to the rights, and to the review.

Segregation of duties is usually discussed as a property of entitlements: no single person should be able to both create a supplier and approve its payment. Access reviews are expected to catch such combinations.

Less often discussed is the segregation inside the review itself. Who designs it, who decides, and who proves it are three different roles. When they collapse into one, the evidence loses its value.

This paper covers both: how to bring conflicting combinations in front of a decision-maker, and how to organise the review so that no one is judge of their own access.

Conflicting combinations
Rights that are harmless alone, dangerous together.

Three roles
Design, decide, prove: never the same hands.

Administration never decides
Those who run the review do not take its decisions.

No self-review
Nobody confirms their own access or privilege.

CONTENTS

01 Separation as a principle
02 Conflicts in the access you review
03 Three roles in every review
04 Administration never decides
05 No self-review
06 Where to start

CHAPTER 01

Separation as a principle

No single person should control a process end to end.

Segregation of duties divides a sensitive process among several people, so that no one can carry it out alone, by error or by intent. It appears in every control framework: ISO 27001 and the SOC 2 criteria both mention it alongside least privilege, and NIS2's implementing regulation names it among the principles for assigning rights.

In access governance, the principle applies at two levels: the rights people hold, and the way those rights are reviewed.

Segregation of duties DEFINITION
the division of a sensitive process among several people, so that no single person can complete it alone.

CHAPTER 02

Conflicts in the access you review

Harmless alone, dangerous together.

A classic conflict combines two rights that are each legitimate: creating a supplier and approving payments; developing code and deploying it to production; administering a system and auditing its logs.

A review that shows each right on a separate line, to separate reviewers, will approve both. The conflict only becomes visible when the combination is presented as such, to someone with the authority to accept it, reduce it or compensate it with another control.

Create and approve
A supplier, a payment, a change.

Build and release
Code written and deployed by the same hands.

Administer and audit
Managing a system and reviewing its trail.

Request and grant
Asking for access and approving it.

CHAPTER 03

Three roles in every review

Design, decide, prove. Never the same hands.

Every access review involves three distinct activities, and each should belong to a different role.

ROLE	WHAT IT DOES, AND WHAT IT NEVER DOES
Administration	Designs and runs the review: scope, policies, calendar, reminders. It never records a decision.
Reviewers	Decide, line by line, with a justification. They never decide on their own access.
Auditors	Consult, verify and export the evidence, read-only. They never run a campaign or decide.

CHAPTER 04

Administration never decides

Those who run the review do not take its decisions.

The most common collapse of roles is the administrator who, faced with an unfinished campaign, closes the remaining lines on behalf of absent reviewers. The campaign completes; the evidence now shows decisions taken by the one person who should not take them.

The safeguard is structural: administrators, whether of a delegated workspace or of the whole subscription, cannot record a review decision at all. Absences are handled by fallbacks and escalation to other reviewers, never by the administrator stepping in.

Structural safeguard DEFINITION
a rule enforced by the system itself, so that it cannot be bypassed by a policy exception or a busy afternoon.

CHAPTER 05

No self-review

Nobody is judge of their own access.

The second collapse is the reviewer who confirms their own rights, or a manager who confirms the access of a close collaborator without independent knowledge. The decision may be right, but it proves nothing.

A review designed for segregation routes a person's own access, and especially their privileges, to someone else: their manager, the owner of the system, or a dedicated team. Where that is impossible, the case is escalated rather than self-approved.

CHAPTER 06

Where to start

Check the review before you check the rights.

Segregation is easiest to improve by examining how the last review was run.

01 **Check who decided in the last campaign,** and whether anyone confirmed their own access.

02 **Separate the three roles** of administration, decision and audit.

03 **Route personal and privileged access** to someone other than the holder.

04 **List the combinations that matter** in your critical processes.

05 **Present conflicts as combinations** to an owner with authority to decide.

REVYCORE

Separate the duties,
and the evidence holds.

Human decisions. Verifiable evidence.

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

revycore.com

This paper describes control principles and the corresponding capabilities of REVYCORE for information purposes; it is neither legal advice nor an audit opinion. Framework references are summarised. © 2026 REVYCORE SAS.