REVYCORE

WHITE PAPER

ISO 27001 & SOC 2.

Access review evidence that holds for the audit.

What the certification audit and the SOC 2 examination expect from user access reviews, and how to evidence them for a point in time and for a whole period.

KNOWLEDGE CENTER

DECEMBER 2026

EXECUTIVE SUMMARY

Neither sets a frequency.

Both test that yours was kept.

ISO/IEC 27001:2022 and the AICPA Trust Services Criteria approach access control from different angles, one as a management system standard, the other as criteria for an examination. On user access reviews, they converge: rights must be granted, reviewed and removed according to a defined policy, and the auditor will test that this happened.

Neither text sets a review frequency. That is left to the organisation's own policy, which then becomes the benchmark. In a SOC 2 Type II, the auditor tests every occurrence over the observation period.

This paper summarises the controls and criteria involved, explains what each audit tests, and describes the evidence that answers both with the same set of records.

ISO 27001, A.5.18
Access rights granted, reviewed, modified and removed per policy.

SOC 2, CC6.2 and CC6.3
Access authorised, removed when no longer needed, reviewed periodically.

Your frequency
Set in your policy; the auditor checks it was met.

One evidence set
The same sealed records serve both audits.

CONTENTS

01 Two frameworks, one discipline
02 ISO 27001: the Annex A controls
03 SOC 2: the CC6 criteria
04 What each audit tests
05 Privileges and segregation
06 One evidence set for both
07 Where to start

CHAPTER 01

Two frameworks, one discipline

The vocabulary differs. The discipline is the same.

ISO 27001 certifies an information security management system. Its Annex A lists controls, several of which concern access. A certification audit, then surveillance audits, check that the controls selected are implemented and effective.

SOC 2 is an examination against the Trust Services Criteria, reported by an independent auditor. A Type I report looks at the design of controls at a point in time; a Type II report looks at their operation over a period, typically six to twelve months.

For user access reviews, both end up asking the same thing: show that rights are reviewed by the right people, at the frequency you committed to, and that what should be removed is removed.

Type II DEFINITION
a SOC 2 report on the operating effectiveness of controls over a period, which requires evidence of each occurrence of a periodic control.

CHAPTER 02

ISO 27001: the Annex A controls

A.9.2.5 did not disappear. It moved into A.5.18.

In the 2022 edition, access control is spread over several Annex A controls. Their purpose is summarised below; the text of the standard is published by ISO.

CONTROL	PURPOSE (SUMMARISED)
A.5.15 Access control	Rules for physical and logical access control are established and applied according to business and security requirements.
A.5.16 Identity management	The full lifecycle of identities is managed.
A.5.18 Access rights	Rights are granted, reviewed, modified and removed in line with the policy. It takes over the former A.9.2.5, review of user access rights.
A.8.2 Privileged access rights	The allocation and use of privileges are restricted and managed.

The standard sets no review frequency. The organisation's access control policy defines it, and the auditor checks that it is met, with evidence.

CHAPTER 03

SOC 2: the CC6 criteria

In a Type II, one review is not enough. It takes all of them.

Logical access is covered by the CC6 criteria of the Trust Services Criteria (2017, points of focus revised in 2022). Their purpose is summarised below; the text is published by the AICPA.

CRITERION	PURPOSE (SUMMARISED)
CC6.1	Logical access security measures protect information assets.
CC6.2	Users are registered and authorised before access is issued, and access is removed when no longer authorised.
CC6.3	Access is granted, modified and removed based on roles and responsibilities, considering least privilege and segregation of duties.
CC6.3, point of focus	The appropriateness of access roles and rules is reviewed periodically.

CHAPTER 04

What each audit tests

The auditor does not read the policy. They test it.

Both audits move quickly from the policy to the records. The questions are the same; the Type II adds the dimension of time.

Did it take place?
A dated occurrence per scope, at the frequency of the policy, and in a Type II, every one over the period.

The right population?
A complete scope, frozen at launch, with justified exclusions.

By whom?
The asset owner, with a justification, not the team that administers it.

And the removals?
Every refused access actually removed, and verified.

CHAPTER 05

Privileges and segregation

The accounts that can change everything deserve their own review.

Both frameworks single out privileged access: ISO 27001 through A.8.2, SOC 2 through the role-based, least-privilege and segregation-of-duties expectations of CC6.3. Privileged accounts are few and powerful; reviewing them in a dedicated policy, at their own pace, is the reading auditors expect.

Segregation of duties applies to the review itself. The person who grants an access should not be the only one who confirms it, and an administrator should never approve their own privileges.

- **A dedicated policy.** Privileged access reviewed separately, often more frequently.
- **No self-approval.** Decisions on a privilege are never taken by its holder.
- **Exceptions in time.** Any exception carries a reason, an owner and an end date.

CHAPTER 06

One evidence set for both

Seal once. Answer both auditors.

Organisations that hold both an ISO 27001 certificate and a SOC 2 report often run their access reviews twice, or document them twice. There is no need: the evidence each auditor wants is the same set of records.

For each campaign, the sealed package contains the decisions, the reviewers, the timestamps and the frozen scope, and is verified offline, without an account. Refusals are tracked until a later collection confirms the removal. The auditor can be given read-only access, bounded in time, to consult, sample and export.

Between two campaigns, continuous assurance can detect significant changes and call on the right decision-maker without waiting for the next review, which shortens the window an auditor would otherwise question.

CHAPTER 07

Where to start

Write the frequency down. Then keep it.

The fastest route to a clean access review finding is to align the policy, the calendar and the evidence.

01 **State the review frequency** per scope in your access control policy.

02 **Separate privileged access** into its own review, at its own pace.

03 **Freeze each population at launch** and justify every exclusion.

04 **Track removals to verification** and keep exceptions temporary.

05 **Keep one sealed evidence set** and open it to both auditors, read-only.

REVYCORE

One discipline,
evidence for both audits.

Human decisions. Verifiable evidence.

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

revycore.com

Controls and criteria are summarised; the text of ISO/IEC 27001:2022 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.