COMPLIANCE MAPPING

ISO 27001 and SOC 2

What AccessRevoke already covers, control by control

August 2026 · Reference document for sales conversations and the website

Everything below describes only what the product actually does automatically: detects a Joiner/Mover/Leaver event, grants, changes, or removes access, deletes orphaned OAuth tokens, and logs every action to an immutable audit trail. There is no step that waits for human confirmation.

ISO 27001:2022 (Annex A)

What AccessRevoke does automatically	Control	Why it matches
Detects Joiner/Mover/Leaver events	**A.5.16 — Identity management**	The control requires managing the full identity lifecycle — registration, provisioning, maintenance, de-registration.
Grants access on join, via pre-defined role mapping	**A.5.18 — Access rights**	The control is literally triggered by HR events: hiring, role change, termination — role mapping is an approved policy, applied automatically and consistently.
Removes old access + grants new access on internal transfer (Mover)	**A.5.18 — Access rights (modification)**	Directly prevents “privilege creep” — the problem described by the Zühlke interviewee in the research.
Revokes access on departure (Leaver)	**A.5.18 + A.5.15 — Access control**	A.5.15 explicitly cites HR oversight of the leaver process as part of regular access management.
Deletes orphaned OAuth tokens	**A.5.17 — Authentication information**	Covers management of credentials and secrets, not just passwords.
Immutable audit log of every action (grant/revoke/fail)	**A.8.16 — Monitoring activities**	The control requires correlation and analysis of security events to support investigations — the log is direct evidence.

SOC 2 (Trust Services Criteria — Security / Common Criteria)

What AccessRevoke does automatically	Control	Why it matches
Access is granted exclusively via a pre-defined, least-privilege role mapping (not ad hoc requests)	**CC6.1**	Role mapping is the formal authorization — defined once per role, applied consistently to every employee in that role.
Access is removed immediately on a Leaver/Mover event, with no manual step	**CC6.2**	The most direct matching control in this document — CC6.2 literally requires access to be removed promptly upon departure or role change. This is where auditors most often find gaps at companies doing this manually.
Continuous, not periodic, visibility into who currently has what access (Employee directory)	**CC6.3**	The control requires periodic review to remove accounts that are no longer authorized — AccessRevoke does this continuously, which is stronger evidence than a quarterly manual review.
Immutable, timestamped log of every grant/revoke event	**CC7.2**	Exactly what auditors sample — provisioning and termination events, with a trail from request to execution.