Kailash Consult Free resource · kailashconsult.com/resources

SOC 2 Reuse Map

Control by control: which of your SOC 2 evidence already covers ISO 27001:2022 and ISO 42001, and the short list of what is actually new.

How to use

- Start from your current SOC 2 controls and evidence. Each row shows where that work lands in ISO 27001 and ISO 42001.
- Reuse = the same evidence usually works. Extend = keep it, add a little. New = no SOC 2 equivalent.
- References are typical mappings, not a substitute for your auditor's or certification body's view.

Example answers and mappings are templates, not facts about your company. Edit every bracket and validate each statement before sharing it with a customer or auditor.

Common Criteria you already run

ID	SOC 2 area	What you already have	ISO 27001:2022	ISO 42001	Reuse	What to add
M01	CC1 Control environment	Code of conduct, org chart, roles, hiring and accountability.	Clause 5.1, 5.3; A.5.2, A.5.4, A.6.1, A.6.2, A.6.4	Clause 5.3, A.3	Extend	Name ISMS roles and responsibilities; for 42001, add AI roles.
M02	CC2 Communication and information	System description, internal and customer communication.	Clause 7.4; A.5.14, A.5.37	Clause 7.4, A.8	Reuse	Record what you communicate, to whom and when.
M03	CC3 Risk assessment	Annual risk assessment and risk register.	Clause 6.1.2, 8.2	Clause 6.1.2, 6.1.4	Extend	Add a risk treatment plan; for 42001 add AI risks and an AI system impact assessment.
M04	CC4 Monitoring activities	Control monitoring and deficiency tracking.	Clause 9.1, 10.2	Clause 9.1, 10.2	Extend	Add a formal internal audit and management review (see New section).

Kailash Consult

ID	SOC 2 area	What you already have	ISO 27001:2022	ISO 42001	Reuse	What to add
M05	CC5 Control activities and policies	Approved policy set.	A.5.1, A.5.37	Clause 5.2, A.2	Reuse	Map policies to Annex A; for 42001 add an AI policy.
M06	CC1.4 / CC2.2 Training	Security awareness training records.	A.6.3; Clause 7.2, 7.3	Clause 7.2, 7.3	Reuse	For 42001, add AI awareness and competence.
M07	HR screening and exits	Background checks, confidentiality terms, offboarding.	A.6.1, A.6.2, A.6.5, A.6.6	-	Reuse	None, if evidence is current.

Access, systems and operations

ID	SOC 2 area	What you already have	ISO 27001:2022	ISO 42001	Reuse	What to add
M08	CC6.1 Logical access	SSO, MFA, role-based access.	A.5.15, A.5.17, A.8.2, A.8.3, A.8.5	-	Reuse	None, if evidence is current.
M09	CC6.2 / CC6.3 Provisioning and reviews	Access requests, removals, quarterly reviews.	A.5.16, A.5.18	-	Reuse	None, if evidence is current.
M10	CC6.4 Physical access	Cloud provider reports; office controls.	A.7.1 to A.7.4	-	Reuse	Include offices only if they are in ISMS scope; A.7.4 monitoring is new in 2022.
M11	CC6.5 Asset disposal	Device wipe and disposal records.	A.7.14, A.8.10	-	Reuse	Add information deletion procedure (A.8.10).
M12	CC6.6 Boundary protection	Firewalls, security groups, private networks.	A.8.20, A.8.21, A.8.22	-	Reuse	None, if evidence is current.
M13	CC6.7 Data in transit	TLS configuration, transfer controls.	A.5.14, A.8.24	-	Reuse	None, if evidence is current.
M14	CC6.8 Malware and software control	EDR or anti-malware, MDM.	A.8.7, A.8.19	-	Reuse	None, if evidence is current.
M15	CC7.1 Vulnerability and configuration	Scans, patching, configuration checks.	A.8.8, A.8.9	-	Extend	Document configuration baselines (A.8.9 is new in 2022).
M16	CC7.2 Monitoring and logging	Central logs and alerts.	A.8.15, A.8.16	A.6 (AI logging)	Extend	Monitoring activities (A.8.16) is new in 2022; for 42001 log AI events.

Kailash Consult

ID	SOC 2 area	What you already have	ISO 27001:2022	ISO 42001	Reuse	What to add
M17	CC7.3 to CC7.5 Incident response	IR plan, incident tickets, tabletop.	A.5.24 to A.5.28	A.8 (AI incident communication)	Reuse	Keep lessons learned and evidence collection records.
M18	CC8.1 Change management	Pull requests, approvals, CI/CD.	A.8.25, A.8.28, A.8.29, A.8.31, A.8.32	A.6 (AI life cycle)	Extend	Secure coding (A.8.28) is new in 2022; for 42001 add model and prompt changes.
M19	CC9.1 Business disruption	BC/DR plan, backups, restore tests.	A.5.29, A.5.30, A.8.13, A.8.14	-	Extend	ICT readiness for business continuity (A.5.30) is new in 2022.
M20	CC9.2 Vendor management	Vendor reviews and contracts.	A.5.19 to A.5.23	A.10	Extend	Cloud services security (A.5.23) is new in 2022; for 42001 cover AI providers.

Optional SOC 2 categories

ID	SOC 2 area	What you already have	ISO 27001:2022	ISO 42001	Reuse	What to add
M21	A1 Availability	Capacity, backups, redundancy.	A.8.6, A.8.13, A.8.14	-	Reuse	None, if evidence is current.
M22	C1 Confidentiality	Classification and confidential data handling.	A.5.10, A.5.12, A.5.13, A.8.10	A.7	Extend	Add labelling (A.5.13); data masking (A.8.11) and DLP (A.8.12) are new in 2022.
M23	P Privacy	Privacy notice and personal data handling.	A.5.34	A.7	Reuse	None, if evidence is current.

New for ISO 27001 (no SOC 2 equivalent)

ID	SOC 2 area	What you already have	ISO 27001:2022	ISO 42001	Reuse	What to add
N01	Context and interested parties	-	Clause 4.1, 4.2	Clause 4.1, 4.2	New	Document internal and external issues and what interested parties require.
N02	ISMS scope	-	Clause 4.3	Clause 4.3 (AIMS scope)	New	Write the scope: products, locations, teams, systems.

Kailash Consult

ID	SOC 2 area	What you already have	ISO 27001:2022	ISO 42001	Reuse	What to add
N03	Risk treatment and Statement of Applicability	-	Clause 6.1.3	Clause 6.1.3	New	Decide applicability of all 93 Annex A controls with reasons.
N04	Security objectives	-	Clause 6.2	Clause 6.2	New	Measurable objectives with owners and dates.
N05	Control of documented information	-	Clause 7.5	Clause 7.5	New	Version, approval and access rules for ISMS documents.
N06	Internal audit	-	Clause 9.2	Clause 9.2	New	An independent internal audit before certification.
N07	Management review	-	Clause 9.3	Clause 9.3	New	Leadership reviews ISMS performance; keep minutes.
N08	Controls added in ISO 27001:2022	-	A.5.7, A.5.23, A.5.30, A.7.4, A.8.9, A.8.10, A.8.11, A.8.12, A.8.16, A.8.23, A.8.28	-	New	Threat intelligence, cloud security, ICT readiness, physical monitoring, configuration, deletion, masking, DLP, monitoring, web filtering, secure coding.
N09	Certification audit	-	Stage 1 and Stage 2 by an accredited certification body	Same for ISO 42001	New	Three-year certificate with annual surveillance audits.

New for ISO 42001 (AI management system)

ID	SOC 2 area	What you already have	ISO 27001:2022	ISO 42001	Reuse	What to add
N10	AI policy and objectives	-	-	Clause 5.2, 6.2, A.2	New	AI policy approved by leadership, with measurable AI objectives.
N11	AI risk and impact assessment	-	-	Clause 6.1.2, 6.1.4, A.5	New	Assess risks and impacts of each AI system on people and the business.
N12	AI system inventory and life cycle	-	-	A.6	New	Inventory of AI systems with design, testing, release and monitoring records.

Kailash Consult

ID	SOC 2 area	What you already have	ISO 27001:2022	ISO 42001	Reuse	What to add
N13	Data for AI	-	-	A.7	New	Data quality, provenance and preparation records for AI data.
N14	Information for interested parties	-	-	A.8	New	User documentation, transparency and AI incident communication.
N15	Responsible use of AI	-	-	A.9	New	Intended use, human oversight and acceptable use rules.
N16	Third-party and customer relationships	-	-	A.10	New	AI supplier assessment and customer responsibilities.

Free resource from Kailash Consult. Free to use inside your company. Not for resale or redistribution. kailashconsult.com/resources

Kailash Consult