

SOC Engagement Preparation Tracker

Version 1.0 · Updated October 8, 2026 · Preparation aid; adapt to your firm's methodology

A preparation tracker for SOC 1 and SOC 2 engagements: engagement type, systems or services and period, contacts, control owners, record sources, request status and follow-up, with the SOC 1 / SOC 2 and Type 1 / Type 2 distinctions stated briefly.

Audience: SOC and assurance teams planning fieldwork; the professional firm sets the applicable criteria.

AuditPartners / auditpartners.com

How to use

1. Complete the engagement rows first (type, systems or services, period, contacts). Then use one row per control area or request.
2. SOC 1 covers controls relevant to user entities' financial reporting; SOC 2 covers the Trust Services Criteria the service organization selects. Type 1 describes design at a point in time; Type 2 also covers operating effectiveness over a period. The engagement firm decides what applies.
3. Record owners, record sources and request status. Do not store client records in this tracker.
4. Report wording, criteria and testing are set by the engagement firm and its standards; this tracker only organizes preparation.

SOC preparation

Engagement rows describe the engagement; area rows track preparation per control area. The first row is a fictional example — overwrite it.

Dropdown columns in the XLSX edition: Request status (Not started / Requested / Partly received / Received / Not applicable).

ID	Item	Detail / what to record	Control owner / contact	Record source	Request status	Follow-up
EXAMPLE	Fictional example — delete this row. Logical access	Access provisioning, review and removal for the payroll platform.	IT director	Identity provider export; ticketing tool	Requested	Confirm the export covers all three environments.
ENG-01	Engagement type	SOC 1 or SOC 2; Type 1 (design at a point in time) or Type 2 (design and operation over a period). Set by the engagement firm.				
ENG-02	System or services in scope	The service, applications, infrastructure and locations the description covers.				
ENG-03	Period or point in time	Review period for Type 2 or the as-at date for Type 1.				
ENG-04	Contacts	Engagement lead at the firm, client coordinator and escalation contact.				
ENG-05	Criteria and subservice organizations	Trust Services Criteria or control objectives selected, and any carved-out or inclusive subservice organizations. Decided by the engagement firm with the client.				

ID	Item	Detail / what to record	Control owner / contact	Record source	Request status	Follow-up
SOC-01	Control environment and risk assessment	Organization chart, policies, risk assessment records and management review minutes.				
SOC-02	Communication and monitoring	Policy acknowledgments, security training records, monitoring reports and issue tracking.				
SOC-03	Change management	Change tickets, approvals, test records and deployment logs for the period.				
SOC-04	Vendor and subservice management	Vendor list, contracts or SOC reports relied on, and review records.				
SOC-05	Logical access	User lists, provisioning and removal records, access reviews and privileged access records.				
SOC-06	Physical and environmental security	Data-center attestations or site access records, where relevant to the system.				
SOC-07	Operations, backup and incident response	Job monitoring, backup logs, restore tests, incident records and post-incident reviews.				
SOC-08	Availability, confidentiality, processing integrity, privacy	Records for any additional criteria the client has selected; mark Not applicable where a category is out of scope.				

Worked example (fictional)

Company names and figures are invented.

Fictional example: SOC 2 Type 2, hosted payroll service, 1 January to 31 December

Engagement rows: type SOC 2 Type 2; service 'hosted payroll processing'; period 1 Jan – 31 Dec; contacts: compliance lead and IT director.

SOC-05 (logical access): owner IT director; record source identity provider export and ticketing tool; status Requested; follow-up: confirm the export covers all three environments.

References

AICPA Trust Services Criteria

<https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022>

ISO/IEC 27002:2022 — Information security controls

<https://www.iso.org/standard/75652.html>

IIA Global Internal Audit Standards (2024)

<https://www.theiia.org/en/standards>

Disclaimer

Preparation aid for CPA, SOC, IT and assurance teams — not an audit program, a list of required tests or evidence of compliance. Adapt it to your firm's methodology and professional standards. Record only references and status; do not paste client records into this file or send them through the website. The example row is fictional.