

[Company name]

SOC 2 Evidence Request List

Also called	PBC list (provided by client) or document request list
Report type	[Report type]
Period or date	[Period start] to [Period end], or [As-of date] for a Type 1
CPA firm	[CPA firm]
Requests	73

1. How to use this list

This list gathers, in auditor words, the evidence a SOC 2 examination of [Company name] with the Security category in scope usually asks for, one numbered request per row, in criterion order. [CPA firm] sends its own request list: match its numbers to these rows and add any request that is not here.

Each request has a kind, and the kind decides what it covers in each report type.

Kind	What it covers
Setting	Type 1: as of the report date. Type 2: at points the auditor picks across the period.
Document	Type 1: the version in effect on the report date. Type 2: every version in effect during the period, with its approval.
Population	Type 1: usually one example. Type 2: the full list for the period, then the samples the auditor picks from it.
Recurring event	Type 1: the latest one before the report date. Type 2: each one that fell inside the period.

- Name an owner for every request before fieldwork starts.
- Export populations from the system of record with the filter visible, so the auditor can see the list is complete.
- Show the system and the date in every screenshot.
- Delete the A1 rows if the Availability category is not in scope.

2. Governance, people and communication

No.	Criterion	Code	Evidence requested	Usual source	Format	Kind
1	CC1.1	B4	Code of conduct in effect, with its approval	Document system or wiki	Document	Document
2	CC1.1	B4	Signed code of conduct acknowledgments for the sampled employees and contractors	HR system	Record	Population
3	CC1.1	H2	Non-disclosure agreement template	Contract files	Document	Document
4	CC1.1	H2	Signed non-disclosure agreements for the sampled new hires	HR system	Record	Population
5	CC1.2	B8	Minutes of board or advisory meetings where security was discussed	Board or advisory minutes	Document	Recurring event
6	CC1.3	B3	Organization chart and the list of security roles with their owners	Document system or wiki	Document	Document
7	CC1.4	H1	List of new hires during the period, with start dates	HR system	Export	Population
8	CC1.4	H1	Completed background checks for the sampled new hires, redacted	HR system	Record	Population
9	CC1.4	H3	Security awareness training completion for all personnel	Training platform	Export	Population
10	CC1.4	H4	List of employees and contractors who left during the period, with end dates	HR system	Export	Population
11	CC1.5	B9	Job descriptions or performance expectations that include security responsibilities	HR system	Document	Document
12	CC2.1	R4	Control deficiencies reported to management, with who received them	Ticketing system	Ticket sample	Recurring event
13	CC2.2	B3	Information security policy and how it was published to personnel	Document system or wiki	Screenshot	Document

No.	Criterion	Code	Evidence requested	Usual source	Format	Kind
14	CC2.3	Q2	Customer facing system description and the list of customer responsibilities	Document system or wiki	Document	Document
15	CC2.3	Q2	Customer agreement template with its security commitments	Contract files	Document	Document

3. Risk assessment, monitoring and control activities

No.	Criterion	Code	Evidence requested	Usual source	Format	Kind
16	CC3.1	E1	Most recent risk assessment, with its date and approver	Document system or wiki	Document	Recurring event
17	CC3.2	E2	Risk register with owners, ratings and treatment	Document system or wiki	Export	Document
18	CC3.3	E4	Risk assessment pages or register rows on fraud and insider misuse	Document system or wiki	Document	Document
19	CC3.4	E5	A significant change assessed for risk before rollout	Ticketing system	Ticket sample	Recurring event
20	CC4.1	R1	Minutes of the management review of the security program	Board or advisory minutes	Document	Recurring event
21	CC4.1	M3	Penetration test report or executive summary, with the fixes for its findings	Penetration test provider	Report	Recurring event
22	CC4.2	R2	Remediation tracker for findings from audits, tests and incidents	Ticketing system	Export	Population
23	CC5.1	E1	Mapping of risks to the controls that address them	Document system or wiki	Document	Document
24	CC5.2	M5	Hardening or configuration baseline for production systems	Document system or wiki	Document	Document
25	CC5.2	F6	Inventory of production systems, data stores and SaaS applications with owners	Asset inventory	Export	Setting
26	CC5.3	R1	List of security policies with their approval dates	Document system or wiki	Document	Document

4. Access, data protection and devices

No.	Criterion	Code	Evidence requested	Usual source	Format	Kind
27	CC6.1	G1	Multi-factor authentication enforcement settings for the identity provider and the cloud console	Identity provider, for example Okta or Google Workspace; Cloud console, for example AWS	Screenshot	Setting
28	CC6.1	G1	List of users with their multi-factor authentication status	Identity provider, for example Okta or Google Workspace	Export	Setting
29	CC6.1	G1	Password and session settings	Identity provider, for example Okta or Google Workspace	Screenshot	Setting
30	CC6.1	G4	Production roles and groups, with the members of each	Cloud console, for example AWS	Export	Setting
31	CC6.1	I3	Encryption at rest settings for databases, storage and backups	Cloud console, for example AWS	Screenshot	Setting
32	CC6.1	I1	Data classification standard	Document system or wiki	Document	Document
33	CC6.2	G8	User lists from each in-scope system	Identity provider, for example Okta or Google Workspace; Cloud console, for example AWS; Code repository, for example GitHub	Export	Population
34	CC6.2	G9	Approved access requests for the sampled new users	Ticketing system	Ticket sample	Population
35	CC6.2	G7	Access removal for the sampled leavers, with the time each account was disabled	Identity provider, for example Okta or Google Workspace; Ticketing system	Ticket sample	Population
36	CC6.2	H4	Completed offboarding checklists for the sampled leavers	HR system	Record	Population

No.	Criterion	Code	Evidence requested	Usual source	Format	Kind
37	CC6.3	G8	Completed user access reviews, with the reviewer, the date and the changes made	Document system or wiki	Record	Recurring event
38	CC6.3	G4	List of people with administrator access to production	Cloud console, for example AWS	Export	Setting
39	CC6.4	C4	The cloud provider's SOC 2 report covering its data centers, with your review of it	Cloud provider compliance portal	Report	Recurring event
40	CC6.5	I10	Data retention schedule and disposal procedure	Document system or wiki	Document	Document
41	CC6.5	I10	Records of customer data deleted at contract end, or of devices wiped	Ticketing system	Record	Population
42	CC6.6	L1	Web application firewall configuration and rules	Cloud console, for example AWS	Screenshot	Setting
43	CC6.6	L1	Security group or firewall rules for production	Cloud console, for example AWS	Export	Setting
44	CC6.7	I2	TLS configuration or scan result for public endpoints	TLS scanner	Report	Setting
45	CC6.8	F4	Endpoint protection coverage for all company laptops	Device management tool	Export	Setting
46	CC6.8	F4	Device compliance report: disk encryption, screen lock and updates	Device management tool	Export	Setting

5. Operations, monitoring and incidents

No.	Criterion	Code	Evidence requested	Usual source	Format	Kind
47	CC7.1	M1	Vulnerability scan reports	Vulnerability scanner	Report	Recurring event
48	CC7.1	M4	Critical vulnerabilities found during the period, with the date each was fixed	Vulnerability scanner; Ticketing system	Export	Population

No.	Criterion	Code	Evidence requested	Usual source	Format	Kind
49	CC7.1	M5	Configuration scan or infrastructure code showing the baseline applied	Code repository, for example GitHub	Screenshot	Setting
50	CC7.2	K1	Central logging configuration, with the sources collected and the retention	Logging and alerting tools	Screenshot	Setting
51	CC7.2	K3	Alert rules for security events and where each alert goes	Logging and alerting tools	Screenshot	Setting
52	CC7.2	K3	Security alerts raised during the period and how each was handled	Logging and alerting tools; Ticketing system	Ticket sample	Population
53	CC7.3	O1	Incident response plan, with its approval	Document system or wiki	Document	Document
54	CC7.3	O1	List of security incidents during the period	Ticketing system	Export	Population
55	CC7.4	O1	Incident records for the sampled incidents, from detection to closure	Ticketing system	Ticket sample	Population
56	CC7.4	O1	Record of the incident response exercise or tabletop	Document system or wiki	Document	Recurring event
57	CC7.5	O3	Root cause analysis for each high severity incident	Document system or wiki	Document	Recurring event
58	CC7.5	P1	Backup configuration: frequency, retention and location	Cloud console, for example AWS	Screenshot	Setting

6. Change management

No.	Criterion	Code	Evidence requested	Usual source	Format	Kind
59	CC8.1	N1	Change management policy	Document system or wiki	Document	Document
60	CC8.1	N1	List of production changes during the period	Code repository, for example GitHub; deployment pipeline	Export	Population
61	CC8.1	N2	Branch protection settings that require review before merge	Code repository, for example GitHub	Screenshot	Setting

No.	Criterion	Code	Evidence requested	Usual source	Format	Kind
62	CC8.1	N2	Pull requests for the sampled changes, showing review and approval	Code repository, for example GitHub	Ticket sample	Population
63	CC8.1	N5	Deployment approvals for the sampled releases	Deployment pipeline	Ticket sample	Population
64	CC8.1	N3	Diagram or settings showing development, test and production are separated	Cloud console, for example AWS	Screenshot	Setting
65	CC8.1	N4	Emergency change procedure, and each emergency change made	Document system or wiki; Ticketing system	Document	Recurring event

7. Vendors, continuity and availability

No.	Criterion	Code	Evidence requested	Usual source	Format	Kind
66	CC9.1	P5	Business continuity and disaster recovery plan	Document system or wiki	Document	Document
67	CC9.1	P5	Disaster recovery test results	Document system or wiki	Report	Recurring event
68	CC9.2	Q3	Vendor register with criticality and last review date	Vendor register	Export	Setting
69	CC9.2	Q1	Security reviews for the sampled critical vendors	Vendor register	Record	Population
70	CC9.2	Q1	Contracts with critical vendors, showing their security terms	Contract files	Document	Population
71	CC9.2	C4	Review of each subservice organization's SOC 2 report, with its complementary controls mapped	Vendor register	Document	Recurring event
72	A1.2	P1	Backup job history for the period (Availability only)	Cloud console, for example AWS	Export	Population
73	A1.3	P5	Restore test records (Availability only)	Document system or wiki	Record	Recurring event

8. Tracking status

Give every request one status at a time. The Excel version has the same statuses in a list on each row, and a status tracker for dates and follow ups.

Status	Meaning
Not started	Nobody has collected it yet.
In progress	The owner is collecting it.
Provided	Uploaded or sent to the auditor.
Follow up asked	The auditor asked a question or wants more. Note what in the status tracker.
Accepted	The auditor has what it needs for this request.

9. Fields to complete

Replace every bracketed field in this document with your own detail, then delete this section.

Field	What to enter
[Company name]	Your legal company name.
[As-of date]	For a Type 1 report, the single date the description speaks about.
[Period start]	For a Type 2 report, the first day of the period.
[Period end]	For a Type 2 report, the last day of the period.
[Report type]	Type 1 or Type 2, as the report states it.
[CPA firm]	The firm that issued, or is performing, the examination, named exactly as on its engagement letter or opinion.

Source

Source: free template from www.polaralabs.com/templates/evidence-request-list (CC BY 4.0).