

SOC 2 Report Review Checklist

Vendor	[Vendor name]
Service used	[Service used]
Reviewed by	[Reviewer]
Review date	[Review date]

1. How to use this checklist

Use this checklist when a vendor sends [Company name] its SOC 2 report. Work through one copy per vendor per report, write the result of each check, log every exception with your judgement on it, and sign the conclusion. Then record the outcome in the vendor register.

A SOC 2 report is an attestation report issued by an independent licensed CPA firm. It speaks for the period or date it covers and for the system it describes, and nothing else. The checks below are about whether the report covers what you rely on the vendor for, and what it leaves for you to do.

Result for each check: Met, Not met, Follow up or Not applicable. A Not met or a Follow up carries a note saying what you did about it.

Reviewing vendor reports this way is one accepted way of assessing vendor risk under CC9.2. A security questionnaire, a contract clause or a call with the vendor can stand beside it or in place of it, as your vendor management policy sets.

2. Report basics

Check	What to look for	Where in the report	Result
Report type	Type 1 tests design on one date. Type 2 tests design and operation over a period, and is the one that shows controls ran.	Title page, Section 1	
Period covered	A Type 2 period, or a Type 1 as-of date, that ended recently enough to rely on.	Title page, Section 1	
Auditor is a licensed CPA firm	The firm named on the opinion letter appears in the license register of a state board of accountancy.	Section 1	
Opinion type	Unqualified, qualified, adverse, or a disclaimer of opinion.	Section 1	

Opinion	What it means
Unqualified	The CPA firm concluded that the description is fairly presented and the controls were suitably designed and, for a Type 2, operated effectively. Exceptions can still appear in Section 4.
Qualified	The same conclusion except for one or more matters the opinion names. Read the basis paragraph and decide whether those matters touch your data.
Adverse	The firm concluded that the description is not fairly presented or the controls did not meet the criteria. Escalate before relying on the vendor.
Disclaimer of opinion	The firm could not obtain enough evidence to form an opinion. The report gives you no assurance.

3. Scope

Check	What to look for	Where in the report	Result
Trust services categories	The categories in scope cover what you rely on the vendor for, for example Availability if you depend on its uptime.	Sections 1 and 3	
Systems in scope	The product and locations you actually use are inside the described system.	Section 3	
Subservice organizations	Each one is named, with the carve out method (its controls excluded) or the inclusive method (its controls included and tested).	Section 3	

4. The opinion letter

Check	What to look for	Where in the report	Result
Signed and dated	Firm letterhead, the city it signed from, a date and a signature.	Section 1	
Modifications	Any paragraph headed basis for qualified opinion, adverse opinion or disclaimer, and what it says.	Section 1	

5. Management assertion

Check	What to look for	Where in the report	Result
Present and consistent	Signed by vendor management, naming the same system, period and categories as the opinion.	Section 2	

6. Exceptions and deviations

Check	What to look for	Where in the report	Result
Exceptions listed	Every test with a deviation in the results. Log each one on the Exceptions log sheet with your judgement.	Section 4	
Management responses	What vendor management says it did about each exception. The auditor usually has not tested these responses.	Section 4 or 5	

Log each exception with the criterion, the control, the exception as the report states it, the vendor response, and your judgement: Acceptable, Acceptable with follow up, Escalate, or Not acceptable. Judge it against what you rely on the vendor for, not against how many exceptions there are.

Ref	Criterion	Exception as reported	Vendor response	Your judgement	Effect on us	Action

7. Complementary user entity controls

Check	What to look for	Where in the report	Result
Complementary user entity controls	The controls the vendor assumes you operate. List each one and who at your company does it.	Section 3	

The vendor designed its controls assuming its customers operate these. If [Company name] does not, the vendor's controls may not achieve what the report says for [Company name] data.

Control the report assigns to you	How we operate it	Owner

8. Subservice organizations

Check	What to look for	Where in the report	Result
Their reports	For each carved out subservice organization, whether you need its own report or rely on the vendor monitoring it.	Section 3	

9. Bridge letter

Check	What to look for	Where in the report	Result
Gap since the period ended	If the period ended more than three months before your review, a bridge letter from vendor management covering the months since.	Separate letter	

A bridge letter is a statement by vendor management, not by the CPA firm, and it gives no assurance. It is still the record of what the vendor says changed since the period ended.

10. Conclusion and sign-off

Conclusion	When to choose it
Accept	Every check met, and no exception touches what you rely on the vendor for.
Accept with follow up	Usable now, with named actions, such as checking an exception in the next report.
Escalate	A qualified opinion, an exception that touches your data, or a scope gap. The approver decides.
Do not rely	An adverse opinion, a disclaimer, a firm you cannot find in a license register, or a report that does not cover the service you use.

Conclusion: [Accept, Accept with follow up, Escalate or Do not rely]. Next review: [Next review].

Reviewer

Name: _____

Signature: _____

Date: _____

Approver

Name: _____

Signature: _____

Date: _____

11. Worked example

Moonrake, a fictional ten person company that sells API security monitoring to fintech companies, reviews the SOC 2 Type 2 report of Lanternfish (lanternfish.dev), the fictional analytics provider behind its dashboard usage data. The workbook carries the same review with every check filled in.

11.1 Review record

Item	Entry
Vendor and service	Lanternfish, product analytics for the Moonrake dashboard
Report	SOC 2 Type 2, the Lanternfish analytics platform, Security and Availability
Period	1 April to 31 March
CPA firm	Named in Section 1 and found in the license register of its state board
Opinion	Unqualified
Reviewed	21 July, by the chief technology officer
Bridge letter	Requested on 21 July and received 28 July. It disclosed one change: access removal is now automated from the human resources system
Conclusion	Accept with follow up, approved by the chief executive officer

11.2 Exceptions and the reviewer judgement

Ref	Criterion	Exception as reported	Vendor response	Judgement	Effect on Moonrake
E1	CC6.2	For 2 of 25 terminated employees sampled, production access was removed 9 and 14 days after termination	Removal is now triggered automatically from the human resources system. Management states neither account was used after termination	Acceptable with follow up	Low. Lanternfish holds usage events keyed by hashed user IDs, not API traffic or credentials
E2	CC8.1	For 1 of 40 changes sampled, the change was deployed without the documented peer review	Branch protection now blocks a merge without an approving review	Acceptable	Low. One change, and the response closes the path it used

11.3 Complementary user entity controls

Control the report assigns to Moonrake	How Moonrake operates it	Owner
User entities manage their own users of the Lanternfish dashboard, including removing people who leave	Lanternfish sign in goes through Okta, and the accounts are in the quarterly access review	Chief technology officer
User entities send only the data their agreement with Lanternfish allows	Moonrake sends dashboard usage events keyed by a hashed user ID, and no customer API traffic	Engineering lead
User entities protect the API keys they use to send events	The key is held in AWS Secrets Manager and rotated once a year	Engineering lead

12. 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.
[Vendor name]	The vendor the questionnaire or report review is about, by its legal name.
[Service used]	What your company uses the vendor for, and what data the vendor holds.
[Reviewer]	The person who works through the checklist, with their role.
[Review date]	The day the review is finished and signed.
[Next review]	When the vendor is reviewed again, for example on receipt of its next report.

Source

Source: free template from www.polaralabs.com/templates/soc-2-report-review-checklist (CC BY 4.0).