

SOC 2 Management Representation Letter

Also called	Rep letter or written representations
Requested by	[CPA firm], at the end of fieldwork
Signed by	[Company name] management, on company letterhead
Dated	[Report date], the same date as the CPA firm report

1. How to use this template

At the end of fieldwork the CPA firm asks management to confirm in writing the things only management can confirm: that it is responsible for the system and its description, that the description is fair, that the controls were designed and operated as described, and that it has told the firm everything relevant. The firm supplies its own wording, and that is the letter management signs.

This template shows what that letter usually contains, so management can prepare before it arrives: gather the incident log, the change records and the list of exceptions, and check each representation against them. It is not a replacement for the letter the firm sends. When the firm letter arrives, read every line of it, not this one, before signing.

The representation letter is different from the management assertion. The assertion is printed in Section 2 of the SOC 2 report and is read by everyone who receives the report. The representation letter is addressed to [CPA firm] only, stays in the firm working papers, and is not part of the report.

This version is for a Type 2 report. For a Type 1, replace "throughout the period [Period start] to [Period end]" with "as of [As-of date]" and delete representation 5.

2. Who writes it, who signs it, and when

Question	Answer
Who asks for it	[CPA firm], the independent licensed CPA firm performing the examination, near the end of fieldwork.
Who writes it	The firm usually supplies the wording. Management puts it on company letterhead.
Who signs it	Members of management responsible for the system and with knowledge of the matters in it, for example the chief executive officer and the officer who owns the controls. Here: [Signer name], [Signer title].
When it is dated	The same date as the CPA firm report. The firm does not issue its report until it has the signed letter.

Question	Answer
Who it goes to	The CPA firm only. It is not sent to customers.

3. The letter

[Company letterhead]

[Report date]

To [CPA firm]

We are providing this letter in connection with your examination of the description of [Company name]'s [System name] system for the period [Period start] to [Period end], and of the suitability of the design and operating effectiveness of the controls stated in the description to provide reasonable assurance that our service commitments and system requirements were achieved based on the trust services criteria relevant to [Categories in scope].

We confirm, to the best of our knowledge and belief, having made the inquiries we considered necessary, the following representations made to you during your examination:

1. We are responsible for the description of [Company name]'s [System name] system (the description) and for preparing and presenting it fairly in accordance with the description criteria. We are also responsible for our assertion, which accompanies the description, and we confirm it as of the date of this letter.
2. We are responsible for designing, implementing and operating controls within the system to provide reasonable assurance that [Company name]'s service commitments and system requirements were achieved based on the trust services criteria relevant to [Categories in scope], for selecting those criteria, and for identifying the risks that threaten the achievement of those commitments and requirements.
3. The description fairly presents the [System name] system that was designed and implemented throughout the period [Period start] to [Period end].
4. The controls stated in the description were suitably designed throughout the period to provide reasonable assurance that our service commitments and system requirements would be achieved if the controls operated effectively.
5. The controls stated in the description operated effectively throughout the period to provide reasonable assurance that our service commitments and system requirements were achieved.
6. We have disclosed to you all deviations in the operation of controls, all security incidents and system incidents, all instances of non-compliance with laws, regulations or contracts, and all fraud or suspected fraud of which we are aware that could affect the description or the controls.
7. We have given you access to all information, records and people you asked for, and we have disclosed all matters relevant to the description and the controls of which we are aware.
8. We have disclosed to you any event after the end of the period, up to the date of this letter, that could have a significant effect on the description or on our assertion.

9. The description identifies each subservice organization the system uses, states whether it is presented using the carve out or the inclusive method, and describes the complementary subservice organization controls and the complementary user entity controls that the controls assume.
10. The changes to the system and its controls during the period, and the matters disclosed to you, are listed in the table attached to this letter, and the list is complete.

[Signer name], [Signer title], [Company name]

[Second signer name and title], [Company name]

Officer signing for management

Name:

Signature:

Date:

Second officer

Name:

Signature:

Date:

4. Attached: changes and matters disclosed

List every change to the system or its controls during the period, and every matter in representation 6 that you disclosed to the firm. If there is nothing to list in a row, write None. A matter disclosed in conversation still goes in the table.

Item	Date	What happened	Control or criterion affected	Disclosed to the firm on
Change to the system or controls				
Deviation in a control				
Security or system incident				
Non-compliance with a law, regulation or contract				
Fraud or suspected fraud				
Event after the period end				

4.1 Worked example

Moonrake, a fictional ten person company on AWS, at the end of its first Type 2 period, would fill the table like this:

Item	Date	What happened	Control or criterion affected	Disclosed to the firm on
Change to the system or controls	7 April	The deployment pipeline moved from a long lived AWS key to short lived credentials	CC6.1, CC8.1	At the walkthrough
Deviation in a control	3 May	One quarterly access review was finished nine days after its due date	CC6.2, CC6.3	When the firm tested the review
Security or system incident	7 April	An AWS key flagged in a pull request, deactivated in 25 minutes, no use found	CC7.3, CC7.4	At the walkthrough, with the incident log
Non-compliance with a law, regulation or contract		None		
Fraud or suspected fraud		None		
Event after the period end	12 August	A breach at the help desk vendor exposed four support tickets	CC9.2, CC7.4	Before the letter was signed

5. What the letter is not

- It is not evidence that a control operated. The firm tests the controls itself, and a representation does not stand in for a record the firm asked for.
- It does not change the opinion. The opinion rests on the evidence the firm obtained, and the letter confirms what management told the firm along the way.
- It is not the management assertion, which is Section 2 of the report and is read by its users.
- It is not a document to send to customers, and it says nothing about the months after the date it is signed.

6. Before you sign

1. Read each representation in the firm letter against the incident log, the change records, the exceptions the firm raised and the list of subservice organizations.
2. Fill in the attached table, and check that every item in it was told to the firm before the letter date.

3. If you cannot make one of the representations as written, tell the firm before signing and let it decide what follows. Do not edit the wording yourself.
4. Sign on the date the firm gives you, which is the date of its report, never earlier.
5. Keep a signed copy with the audit records.

7. 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.
[System name]	The product or service the report covers.
[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.
[Signer name]	The officer signing for management.
[Signer title]	Their title, printed under the name.
[Categories in scope]	For example the Security category.
[CPA firm]	The firm that issued, or is performing, the examination, named exactly as on its engagement letter or opinion.
[Report date]	The date the CPA firm gives its report. The letter carries the same date.
[Second signer name and title]	A second officer who knows the matters in the letter, if the CPA firm asks for one. Delete the line if not.

Source

Source: free template from www.polaralabs.com/templates/management-representation-letter (CC BY 4.0).