[Company name]

Management Assertion Letter

Report	SOC 2 Type 1 or Type 2, Section 2
Written by	[Company name] management
Signed by	[Signer name], [Signer title]
Dated	[Report issue date]

1. How to use this template

This letter is Section 2 of a SOC 2 report. Management writes it, an officer signs it, and it is dated the day the report is issued. Use the Type 1 wording for a report as of a single date, or the Type 2 wording for a report covering a period, and delete the other.

The wording follows the 2018 description criteria (DC section 200) and the trust services criteria (TSP section 100). A Type 1 letter confirms two statements, a and b. A Type 2 letter confirms a third, c, that the controls operated effectively. Delete the user entity paragraph and the complementary controls conditions if your description names no complementary controls.

Name only the trust services categories in your scope. Your CPA firm confirms the final wording against the report it issues. This letter is not the management representation letter, which is addressed to the firm and is never published.

2. Type 1 assertion, as of a date

Assertion of the management of [Company name]

We have prepared the accompanying description of the [System name] system as of [As-of date] (description) based on the criteria for a description of a service organization's system set forth in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (description criteria). The description is intended to provide report users with information about the [System name] system that may be useful when assessing the risks arising from interactions with it, particularly information about system controls that [Company name] has designed and implemented to provide reasonable assurance that its service commitments and system requirements would be achieved based on the trust services criteria relevant to [Categories in scope] (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

> Insert the subservice organization paragraph from section 4 here.

The description also indicates that complementary user entity controls assumed in the design of [Company name]'s controls are necessary, along with controls at [Company name], to achieve [Company name]'s service commitments and system requirements. The description presents those complementary user entity controls and does not disclose the actual controls at the user entities.

We confirm, to the best of our knowledge and belief, that:

a. the description presents the [System name] system that was designed and implemented as of [As-of date] in accordance with the description criteria.

b. the controls stated in the description were suitably designed as of [As-of date] to provide reasonable assurance that [Company name]'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organization and user entities applied the complementary controls assumed in the design of [Company name]'s controls as of that date.

[Signer name], [Signer title], [Company name]. Signed [Report issue date].

Officer signing for management

Name:

Signature:

Date:

3. Type 2 assertion, throughout a period

Assertion of the management of [Company name]

We have prepared the accompanying description of the [System name] system throughout the period [Period start] to [Period end] (description) based on the criteria for a description of a service organization's system set forth in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (description criteria). The description is intended to provide report users with information about the [System name] system that may be useful when assessing the risks arising from interactions with it, particularly information about system controls that [Company name] has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to [Categories in scope] (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

> Insert the subservice organization paragraph from section 4 here.

The description also indicates that complementary user entity controls assumed in the design of [Company name]'s controls are necessary, along with controls at [Company name], to achieve [Company name]'s service commitments and system requirements. The description presents those complementary user entity controls and does not disclose the actual controls at the user entities.

We confirm, to the best of our knowledge and belief, that:

a. the description presents the [System name] system that was designed and implemented throughout the period [Period start] to [Period end] in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period [Period start] to [Period end] to provide reasonable assurance that [Company name]'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of [Company name]'s controls throughout that period.

c. the controls stated in the description operated effectively throughout the period [Period start] to [Period end] to provide reasonable assurance that [Company name]'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of [Company name]'s controls operated effectively throughout that period.

> If a control did not operate as described, use the wording in section 5 for statement c.

[Signer name], [Signer title], [Company name]. Signed [Report issue date].

Officer signing for management

Name:

Signature:

Date:

4. The subservice organization paragraph

Use one of these for each subservice organization the description depends on, and state which method you used.

4.1 Carve out

[Company name] uses [Subservice organization] as a subservice organization. The description includes only the controls of [Company name] and excludes the controls of [Subservice organization]. The description also indicates that certain applicable trust services criteria can be met only if complementary subservice organization controls assumed in the design of [Company name]'s controls are suitably designed and operating effectively, along with the related controls at [Company name]. The description does not disclose the actual controls at the subservice organization.

4.2 Inclusive

The description includes the controls of [Subservice organization] relevant to the system, and those controls were examined.

> The inclusive method commits the subservice organization to providing its own assertion and to being tested beside you. Carve out is the usual choice for a small company.

5. When a control did not operate as described

In a Type 2 report, a deviation is disclosed with a qualifier in statement c of the letter:

c. except for the matter described in Section 4 of this report, the controls stated in the description operated effectively throughout the period [Period start] to [Period end] to provide reasonable assurance that [Company name]'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of [Company name]'s controls operated effectively throughout that period.

Write the qualifier once. The detail belongs in Section 4 and the remediation in Section 5.

6. Who signs

An officer with authority to speak for the company who also knows how the system runs, for example the chief executive, chief technology officer or chief information security officer. The auditor never signs it. If the officer who was meant to sign has left before the issue date, the person holding the office on that date signs on behalf of the company. Do not backdate the letter.

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.

Field	What to enter
[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 issue date]	The day the CPA firm issues the report.
[Signer name]	The officer signing for management.
[Signer title]	Their title, printed under the name.
[Categories in scope]	For example the Security category.
[Subservice organization]	A vendor the system depends on, for example your cloud provider.

Source

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