

[Company name]

SOC 2 Bridge Letter

Also called	Bridging letter or gap letter
Written by	[Company name] management, on company letterhead
Signed by	[Signer name], [Signer title]
Covers	[Bridge period start] to [Letter date]

1. How to use this template

A bridge letter covers the months between the end of your last SOC 2 report period and today. Management writes it on company letterhead and an officer signs it. The CPA firm that issued the report does not write it and does not sign it, because the firm examined only the period its report covers.

Use the letter in section 2 when nothing material changed during the bridge period. When something did change, keep section 2 and replace its two statements with the wording in section 3, and list each change. A letter that names a change plainly is more useful to a reader than one that claims a clean gap, and it is the only honest version.

Date the letter the day the officer signs it, and write a new one for each request rather than sending an old one. Send it with the report it refers to, never in place of it.

For a Type 1 report, replace "covering the period [Period start] to [Period end]" with "as of [As-of date]", and start the bridge period the day after that date.

2. The letter, when nothing material changed

[Company letterhead]

[Letter date]

To the users of [Company name]'s SOC 2 report

Re: SOC 2 bridge letter for the period [Bridge period start] to [Letter date]

[Company name] received a SOC 2 [Report type] report on its [System name] system, relevant to the trust services criteria for [Categories in scope], covering the period [Period start] to [Period end]. The report was issued by [CPA firm], an independent CPA firm, on [Report issue date].

This letter covers the period from [Bridge period start], the day after that report period ended, to the date of this letter (the bridge period).

Management of [Company name] is not aware of any material change to the [System name] system, to the description of that system in the report, or to the controls described in the report, during the bridge period. To the best of management's knowledge and belief, those controls have continued to operate as described during the bridge period.

Management is not aware of any security incident during the bridge period that resulted in unauthorized access to customer data or that significantly impaired [Company name]'s ability to meet its service commitments.

[Company name] has engaged [CPA firm] for its next SOC 2 examination, covering [Next report period], and expects that report in [Expected report window].

This letter is a statement by the management of [Company name]. It is not a report of [CPA firm] or of any other CPA firm. No examination has been performed for the bridge period, and the letter provides no assurance. It does not extend, update or amend the SOC 2 report, which speaks only for the period it covers. This letter speaks as of its date and is not updated after it is signed.

Questions about this letter can be sent to [Security contact].

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

Officer signing for management

Name:

Signature:

Date:

3. When something did change

Replace the two statements in section 2 with the paragraphs below, and keep the rest of the letter. State what happened, when, which control it touched and what you did. Do not state that a change had no effect on the controls. Establishing that is examination work, and no examination covers the bridge period.

3.1 The change statement

Management of [Company name] is not aware of any material change to the [System name] system, to the description of that system in the report, or to the controls described in the report, during the bridge period, other than the changes listed below. For each one, the table gives the date, the control it affected, what [Company name] did, and whether the control was operating as described on the date of this letter. Management has not evaluated, and this letter does not state, whether any change affected the achievement of [Company name]'s service commitments and system requirements. That is a matter for the next examination.

What changed	When	Control affected	What [Company name] did	Operating on the letter date
[Describe the change]	[Date or dates]	[Control and criterion]	[What replaced it, or how the lapse was closed]	[Yes, since a date, or no]

3.2 The incident statement

During the bridge period, [Company name] identified the security incidents listed below. Each was handled under [Company name]'s incident response plan.

Found	What happened	Customer data affected, and how that was established	Status
[Date]	[One or two sentences]	[What the records show, or that it is still being investigated]	[Open or closed, with the date]

3.3 Worked example

A twelve person software company on AWS. Its Type 2 period ended March 31 and the letter is signed August 15. Three changes and one incident belong in the letter, written like this:

What changed	When	Control affected	What the company did	Operating on the letter date
The head of engineering, who held the security owner role, left the company	May 12	Security roles (CC1.3) and the quarterly access review (CC6.2)	The chief technology officer took the role on May 12 and performed the June access review on June 28	Yes, since May 12
The production database moved from a single instance to a managed cluster in the same region	July 8	Change management (CC8.1) and backups (CC7.5)	The move went through an approved, peer reviewed change ticket. Backups and point in time recovery were enabled on the new cluster on July 8 and a restore test passed on July 22	Yes, since July 8
Endpoint protection was not installed on two new laptops for 19 days	June 3 to June 22	Malware protection on endpoints (CC6.8)	Found by the monthly device report. Agents installed June 22, and onboarding now withholds production access until the agent reports in	Yes, since June 22

Found	What happened	Customer data affected, and how that was established	Status
August 2	An employee entered their password on a fake sign in page. Multi-factor authentication blocked the sign in.	None. The identity provider sign in log shows no successful sign in from the attacker, and the account reached no production system.	Closed August 3. Password reset and the sender blocked.

4. What the letter must not say

- That the CPA firm reviewed, approved or stands behind the bridge period. Do not use the firm logo or paraphrase its opinion.
- That the report is extended, renewed or still current for the bridge period.
- That the company is certified. A SOC 2 report is an attestation report with an opinion, and there is no certificate.
- That a change had no effect on the controls, or that customer data was unaffected, without the records that show it.

- A date later than the day the officer signs.

5. Who signs, and how long it holds

An officer with authority to speak for the company who knows how the system runs, for example the chief executive, chief technology officer or chief information security officer. A security engineer signing for the company makes a weaker letter, and the CPA firm never signs it.

The letter has no fixed expiry. It covers the bridge period it states and speaks as of its date. Each reader decides how long a gap they accept, and when the gap grows long the answer is the next report rather than another letter. Keep a running note of anything that would belong in section 3 as it happens, so the next letter takes minutes rather than a reconstruction from memory.

6. 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.
[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.
[Letter date]	The day the officer signs. The letter speaks as of this date, so never date it ahead.
[Bridge period start]	The day after the report period ended, or the day after the as-of date of a Type 1 report.
[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.
[Security contact]	The role and email address a reader writes to with questions.
[Next report period]	The period the next examination covers, as the engagement letter states it.

Field	What to enter
[Expected report window]	A month or a quarter, written as an expectation. The CPA firm decides when it issues the report.

Source

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