Your Company Name and Logo in Header

SOC 2 type 1 Structure

The SOC2 report structure can vary based on industry, audit criteria, and the auditor used.

There will generally be at least four sections, sometimes five, in the event of a Management Letter.

Here are the sections and their purpose:

-------------------------- Section 1 --------------------------
Management Assertion

This is a letter from company leaders that includes a summary of products and services as well as the structure of IT systems, teams, and controls. It provides the reader with a list of facts and assertions, or statements, made by the company management related to the systems.

-------------------------- Section 2 --------------------------
Auditor’s Opinion

This is the internal or external auditor’s opinion. It generally falls into three types of results.

1 = Unqualified

- This means that the controls tested as part of the report are designed and operating effectively. An unqualified opinion can still have issues and exceptions. When these appear in an unqualified opinion, then the organization and its auditors were able to mitigate or remediate the risks presented by the exceptions, meaning the control in place was deemed effective

2 = Qualified

- A qualified opinion states that a control or controls are not designed and/or operating effectively and that the issues identified are enough to label one or more controls ineffective. Qualified opinions come about frequently and, while not as problematic as an adverse or disclaimer opinion, they do indicate that one or more controls in place will require improvement.

Exceptions can exist as a result of the following:

- Misstatements in the description of the systems or controls
- Deficiency in the design of a control to meet the objective.
- Deficiency in the operating effectiveness of a control.

When a exception occurs, the auditor will state why they qualified their opinion.

3 = Adverse

- This is a sub-optimal outcome. The auditor will report the company's systems and controls can't be trusted. The auditor will state points of failure similar to that of a qualified opinion.

------------------------- Section 3 -------------------------
Systems Description

This is a detailed system description.
It should do it's best to describe the following:

- Company background
- Overview of the systems used to deliver or maintain any product or service
- Key features of the systems
- Principle service commitments and system requirements
- System boundaries
- Trust Service Criteria not applicable to the systems
- Subservice organizations
- Relevant aspects of the control environment, risk assessment, information, communications, and monitoring
- Incidents and system changes

- Complementary User Entity Controls

special note; Complementary User Entity Controls or CEUC are controls that you, as a service provider want your customers to have in place in order for them to properly use your service. A good example of this is an API, as described in the book.

------------------------- Section 4 -------------------------
Description of Controls

This section is a detailed list of controls and test results if a SOC 2 type 2 audit is performed. This includes any applicable trust service categories, test criteria, any related controls, and tests of controls.

------------------------- Section 5 -------------------------
Management's Response to Exceptions (if applicable)

This is an optional section in response to any findings in the audit requiring explanation of an exception by the company management.

This can include the following types of information:

- Incidents and system changes
- The company's future plans for new systems
- Key aspects of the control environment not covered in the report that the company wants to communicate to its customers or business partners
- A detailed explanation of the company's response to a qualified op[inion