COSMOS
Navigate the Compliance Universe

CEP Magazine - January 2023

Wesley Van Zyl (wesley@scytale.ai) is a Compliance Success Senior Manager for Scytale in Johannesburg, Gauteng, South Africa.

Beginner's guide to SOC 2, Part 2

By Wesley Van Zyl

In Part 1, we discussed the first phase an organization is advised to undergo to have a successful audit and attain SOC 2 compliance, including the first three steps of the audit-readiness process.[1] As a reminder, there are many stages and responsibilities in a SOC 2 process, but they can generally be broken down into the following six key steps:

1. Consider finding a SOC 2 consultant or partner
2. Identify your scope
3. Perform the gap analysis
4. Gather evidence for each control
5. Perform the audit
6. Review the SOC 2 report

In Part 2, we continue to dive in with the next half of the SOC 2 compliance process, covering steps 4–6.

Gathering evidence for each control

By now, you should have:

1. Defined your scope and know what Trust Service Criteria to include.
2. Selected a Type 1 or Type 2 audit and decided on the audit period if a Type 2 review is being performed.
3. Completed the gap analysis and addressed the gaps by implementing all the relevant controls to address the SOC 2 criteria for the in-scope Trust Service Criteria.

Now, the evidence-gathering period in the SOC 2 project can be defined as the period before the auditor arrives to do the actual audit review. For example: if the audit period is established to be January 1 to June 30, this means the auditor will arrive towards the end of June or the beginning of July to perform the audit. This gives the team six months to gather the evidence before the auditor arrives. All controls that have been scoped for the SOC 2 audit need proof to show that the controls are (1) designed and implemented and (2) operating effectively. If a Type 1 audit is being performed, then the evidence is only needed for the first point. If a Type 2 audit is being performed, then evidence will be required for both points.

Obtaining evidence regarding the design and implementation of controls

Design and implementation of the controls are normally tested together. It is important that the evidence clearly shows the auditors that the controls management is in place and implemented as management says they are. Management cannot say they have antivirus software installed on all end users' laptops, and then on the first laptop that is checked, the auditors find the software is not installed. Failing a control on design and implementation is a much more significant deficiency than failing a control on an operating effectiveness level—which is discussed below.

Obtaining evidence regarding the operating effectiveness of controls

As mentioned above, when providing a Type 2 report, the auditor will test those controls that the auditor has determined are necessary to achieve the criteria stated in the service organization's description of its system. The auditor will also assess the operating effectiveness of those controls throughout the period, which must be at least three months and at most 12 months.

When testing for operating effectiveness, the auditor needs to select a sample throughout the period and obtain evidence for the sample to ensure the control was operating effectively throughout the testing period. Using the antivirus example, the auditor will not only ask for one user's laptop but select a sample of laptops.

Evidence provided for the sample selected can range from screenshots to emails to physical documentation. In essence, the evidence provided needs to clearly indicate that the control is being performed as designed over a period of time. In a day and age where almost all the evidence will be electronic, it is important the pieces of evidence have a date stamp. Evidence that does not have a date stamp can provide difficulties for the auditor in determining the evidence's validity.

Evidence obtained in prior audits about the satisfactory operation of controls in previous periods does not provide a basis for a reduction in testing—even if it is supplemented with evidence obtained during the current period. This means the evidence provided needs to be from the current review period.

Perform the audit

Currently, a SOC 2 audit process uses the "trust but verify" approach by external auditing teams. The theory behind this approach is that the company needs to provide evidence to match what they are saying about their controls and security posture, and this evidence needs to be tested by the auditors. This approach allows the auditing team to stay independent of pulling the evidence. Before issuing the report, this is the final phase, and all evidence about the controls scoped for the SOC 2 project must be ready. Unsatisfactory evidence or evidence that cannot be provided will be noted as a finding in the SOC 2 report by the auditor. Depending on the severity and number of the results, SOC 2 compliance might not be obtained.

Auditing firms and auditors differ, but they all follow a similar process in performing the SOC 2 audit.

Pre-audit phase: Sampling

The auditors will request the control list before commencing the audit. From the control list, they will determine which controls a sample selection will be needed if a Type 2 audit is being performed. The auditor will send the samples to management to gather the required evidence before the auditor arrives. The most common lists of information from which auditors select their samples are:

- List of all changes

- List of new employees
- List of terminated employees
- List of board meeting minutes
- List of management minutes
- List of endpoints

Background of the company

On the first day of the audit, management will need to give some background of the company, what product or service offerings are part of the SOC 2 scope, and other information that may offer context to the auditors. This is normally a "get to know" each other phase between the auditor, management, and consultant.

Control and evidence review

This phase is the most significant. This is where the auditor will review the control design, implementation, and operating effectiveness (if a Type 2 audit was requested). This includes the review of the samples selected by the auditor before commencing the audit. The auditor will start from the top and review the evidence for each control from the control list. Some controls will need more explanation than others, which is why it is important to be able to explain the process supporting the evidence that was prepared.

Queries and feedback

At this point, the auditor is documenting their working papers, based on the evidence provided for each control and concluding on each of the controls. Any queries or outstanding items are communicated to management and resolved in this audit phase. The auditors will also offer feedback on any open items where more information is needed or on the status of the SOC 2 audit.

System description analysis

The system description is usually given to the auditors before the start of the audit; however, this is only a preference and not a requirement. The system description needs to be ready and provided to the auditors before the SOC 2 report can be prepared.

Reporting

Once all queries have been resolved and the auditor has received all the evidence and the system description, the auditor will start preparing the SOC 2 report.

Review the SOC 2 report

Once the audit has concluded, you should be notified by the auditing team that the audit review has ended, and the SOC 2 report should be finalized within two to four weeks. This phase of the SOC 2 process requires little involvement from management and is mainly covered by the auditor.

A SOC 2 report has four sections and one optional section. This report is a combined effort between management, the auditor, and the consultant; however, the auditor is responsible for developing the report and signing it off before issuing it to the organization.

The five sections in the SOC 2 report

- **Section 1 – Management's assertion letter:** A summary of what services the organization offers and what its components are. There is a standard template for this letter.
- **Section 2 – Independent service auditor report:** Prepared by the auditor in which they give their opinion on the audit performed. A summary of the results of the SOC 2 audit.
- **Section 3 – System description:** The organization provides a detailed system description that includes background on the organization, explains the control environment, and offers a list of controls that will address the SOC 2 criteria.
- **Section 4 - Applicable Trust Service Principles, criteria, related controls, tests of controls, and results of tests:** This section delivers the details of the auditor's work that was performed and, significantly, the results of each control that was tested and whether there were any exceptions or deviations.
- **Section 5 – Other information provided by the organization:** This section is optional. Any information the organization wants to include in the report can be provided in this section and is typically discussed with the auditor at the end of the audit.

The auditor will share a draft report with management so that they can review it and provide comments on anything that requires further clarification or something that management may not agree with. This is normally resolved in a closeout meeting with the auditors. If exceptions or deviations were found in a particular department by the auditing team, it would be best to have that department's manager sit in and discuss potential shortcomings that were found. This will provide a line of communication between the organization's management team, the auditors, and the department manager where the exception or the deviation is found. Once all queries have been resolved, the auditors will issue the final SOC 2 report to management.

Conclusion

After a successful SOC 2 review, annual maintenance of the SOC 2 compliance process is necessary to continue the process effectively and remain compliant. This will involve the following factors:

- Impact of organizational changes on the control environment
- New legislation and compliance requirements
- Changes in business and risks
- Contractual adjustments
- Changing requirements from user organizations (your clients)
- Recommendations from the auditor

The SOC 2 report is not just a tool for meeting requirements; it is usually the single best description of the information security of your supporting processes, controls, and procedures.

Takeaways

- Design and implementation of the controls are usually tested together.
- All controls that have been scoped for the SOC 2 audit need evidence to show that the controls are (1)

designed and implemented and (2) operating effectively.

- A SOC 2 audit process uses the "trust but verify" approach by external auditing teams.
- The auditor is responsible for developing the report and signing it off before issuing it to the organization.
- The SOC 2 report is not just a tool for meeting requirements; it is generally the single best description of the information security of your supporting processes, controls, and procedures.

1 Wesley Van Zyl, "Beginner's guide to SOC 2, Part 1," *CEP Magazine*, December 2022, https://compliancecosmos.org/beginners-guide-soc-2-part-1.