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.