



VENDOR RISK MANAGEMENT WITH SOC 2 REPORTS

April 2021 Issue Brief

Thorough SOC 2 reports are a valuable tool for vendor risk management. There are twelve key elements for a customer (user entity) to consider as part of reviewing vendor (service provider) reports.

SOC 2 reports contain detailed information that can help you monitor vendor security and compliance and target your efforts when you determine additional diligence is required. Reviewing vendor reports in a methodical way will increase the benefit you get from the reports.

Twelve key elements for consideration

1) Scope of services included

Sometimes a report will cover one specific service, a set of services, or multiple sets of services.

Questions to consider:

- ◆ What service(s) does the report cover?
- ◆ Does that include the specific service(s) used by your organization?

2) Report type

Type 2 reports cover the description, design and operating effectiveness of controls over a period of time.

Type 1 reports, which are common for a new service or first time audit, cover the description and design of controls as of a point in time.

Questions to consider:

- ◆ Is the report a Type 1 or Type 2 report?
- ◆ If it is a Type 1 report, you may want to confirm when the first Type 2 report is expected to be available.

3) Period of coverage

For many organizations, SOC 2 Type 2 examinations are completed annually with reports covering consecutive 12 month periods. In some cases, organizations complete reports covering consecutive 6 month periods or overlapping 12 month periods where more frequent reporting is required.

For an initial SOC 2 Type 2 examination, an organization might cover a shorter period such as 3 or 6

months to enable earlier completion of the report. They would then typically cover a 12 month period of time on a go forward basis.

Questions to consider:

- ◆ What period of time is covered by the SOC 2 Type 2 report?
- ◆ How well does that period align with the period of time you are evaluating?
- ◆ If there is a significant gap between the end of the reporting period and your review date, you may consider obtaining additional information such as a “bridge letter” from the service provider.

4) Categories of criteria

SOC 2 examinations are performed based on the Trust Services criteria which are organized into five categories, four of which are optional.

- The security / common criteria are the required baseline.
- The incremental availability, confidentiality, processing integrity and privacy categories of criteria are optional.
- SOC 2 plus reporting also supports the inclusion of additional external criteria such as the HIPAA security requirements and the Cloud Security Alliance Cloud Controls Matrix requirements.

For cloud providers, it is most common to cover security, availability and sometimes confidentiality.

- Sometimes an organization will cover security in their initial SOC 2 examination and add other categories over time.
- Availability adds coverage of relevant business continuity/disaster recovery controls.
- Confidentiality gives added emphasis to the protection of confidential business information and covers relevant data retention/disposal controls.





Processing integrity can cover a wide range of system processing but is less common in SOC 2 reports because transaction processing controls are more often covered in a separate SOC 1 report.

SOC 2 privacy (and other privacy program certifications) are gaining interest given the rapid expansion of regulatory and contractual requirements and expected increases in regulatory enforcement related to privacy. SOC 2 privacy examinations will be discussed in a future post.

In addition, SOC 2 plus reports can provide broader coverage by addressing additional external frameworks or requirements.

Questions to consider:

- ◆ Which categories of criteria are included in the SOC 2 report?
- ◆ Do those categories align with your business or contractual requirements?
- ◆ If additional coverage would be beneficial to vendor risk management, you may consider conveying that to the service provider.

5) Audit firm

Consideration should be given to the firm that performed the SOC 2 examination.

Questions to consider:

- ◆ Are you familiar with the firm that performed the SOC 2 audit and are they known for performing high quality SOC 2 examinations?
- ◆ If you are unfamiliar with the firm, you may consider researching them and factor that into your evaluation of the thoroughness of the controls and test procedures discussed in element #10 below.

6) Audit opinion

The auditor's opinion is the most important component of the report, specifically the opinion paragraph.

- In the ideal situation, the report has an unqualified opinion, meaning the controls were described, designed and operating effectively to meet the criteria that were in scope.
- In certain cases, the opinion may be qualified, meaning that the criteria were met except for one or more issues called out in the opinion.
- Rarer cases, such as a scope limitation or an adverse opinion due to pervasive control issues, are beyond the scope of this post.

Questions to consider:

- ◆ Was the opinion unqualified or qualified?
- ◆ If the opinion was qualified, you will want to review management's response to the issues, generally included in section V of the report. You may want to consider additional discussion and due diligence with the service provider, depending on the nature and severity of the issues.

7) Treatment of subservice organizations

It is very common for a service provider to use subservice providers that are carved out of the scope of the audit. Subservice providers could include cloud infrastructure, colocation data center, managed security, code repository and various other types of services.

The opinion should indicate any subservice providers that are carved out and the narrative portion of the report (section III) should indicate their control responsibilities in the complementary subservice organization controls (CSOC) section.

The report should also include the service provider's controls to monitor their subservice providers, which typically includes periodic review of their audit reports. In some cases, it might be desirable to also obtain the SOC 2 report from higher impact subservice providers.

A subservice organization may also be included in scope with its controls described and tested in the report in special cases (e.g., where a related entity is providing services to the service provide or if a subservice provider is providing highly customized services).

Questions to consider:

- ◆ What subservice organizations are carved out in the opinion and narrative portion of the report?
- ◆ How does the service provider monitor its subservice providers?
- ◆ Should we consider obtaining a SOC 2 report from one or more higher impact subservice providers with significant CSOC responsibilities?

8) Complementary user entity controls and user entity responsibilities

The report may include complementary user entity controls (CUECs) and/or user entity responsibilities (UERs). CUECs are controls that are expected to be implemented by the customer to achieve the criteria. UERs are items for which the customer is responsible but are not explicitly required for achievement of the criteria. Though the distinction is sometimes subtle, customers should review both and consider their applicability and how they are substantially addressed.

Questions to consider:

- ◆ Does the report specify CUECs and/or UERs?
- ◆ Are they applicable to us and substantially consistent with our controls?

9) Test results, incident disclosures, and management response to exceptions

Type 2 reports include the service provider's controls, the auditor's test procedures, and test results in tabular format in section IV. Type 1 reports do not include the detailed test procedures and results as operating effectiveness is not covered.

It may be the case that there were no occurrences of specific events necessitating a control to operate during the audit period. This is not considered an exception but would be noted in the test results for informational purposes. This is more likely to occur when a report covers less than 12 months of activity.

In addition, SOC 2 requires the disclosure of any significant "system incidents" that impact achievement of service commitments and system requirements based on the Trust Services criteria. This would normally appear in the narrative portion of the report. Incidents of this nature are likely to have an impact on the overall test results as well.



Questions to consider:

- ◆ Were any exceptions (deviations) noted in the report and what was the nature of such exceptions?
- ◆ Were any significant system incidents noted in the narrative portion of the report and what was the nature of such system incidents?
- ◆ Was a management response to each exception (and system incidents if applicable) included in section V of the report?
- ◆ Do we feel management's activities to mitigate the risk or plans to take corrective action are reasonable?

10) Thoroughness of the controls and test procedures

SOC 2 Type 2 reports should include clearly written controls accompanied by specific test procedures. While many controls can be deemed applicable to multiple criteria, it is good practice to avoid excess duplication of controls or the report can become bloated.

To be thorough, testing should emphasize observation of specific control processes and inspection of audit evidence for selections of events/activities and corresponding actions taken or approvals. Testing should not lean too heavily on inquiry of management and inspection of policies and procedures.

Questions to consider:

- ◆ Do the controls listed in the section IV of the report appear reasonable to suit our needs? Are the controls relatively specific and not excessively generic or repetitive?
- ◆ Do the auditor tests appear reasonable to suit our needs (i.e., including tests involving inspection of selections/samples of items, inspection of configurations, observations of certain activities - for all or most controls as opposed to excessive reliance on inquiry and review of policies/procedures)?

11) Service commitments and system requirements

The SOC 2 report ultimately provides an opinion as to whether the service provider achieved its described service commitments and system requirements (relevant to a broad set of customers) based on the Trust Services criteria. Inclusion of the service provider's service commitments and system requirements in the narrative portion of the report has been a requirement since SOC 2 was updated a few years ago. Some organizations include relatively general text whereas others are more specific.

Questions to consider:

- ◆ Does the service commitments and system requirements appear reasonable based on what you have contracted?
- ◆ Do you have significant unique, custom requirements that you may need to separately consider?

12) Other useful information

Section V of the SOC 2 report will sometimes include other useful information such as mappings of the SOC 2 controls to other relevant frameworks and standards that are applicable to customers.

Questions to consider:

- ◆ Consider whether any such information is included and helpful.

Documentation of vendor review

In completing and evidencing your review of a service provider's SOC 2 report, you should consider documenting the following:

- ◆ Review of the elements listed above
- ◆ Your overall conclusion from the review
- ◆ Identified action items
- ◆ Expected date of the next SOC 2 report for follow up purposes
- ◆ Reviewer signoff and date.



For More Information



Mark Lundin

Cloud, Security and Privacy Assurance

Email: connect@lundin.net

LinkedIn: [linkedin.com/in/lundinmark](https://www.linkedin.com/in/lundinmark)

Blog: cloudsecurityprivacy.com



CLOUD, SECURITY AND PRIVACY ASSURANCE BLOG

cloudsecurityprivacy.com