Southern Illinois University

Service Provider Internal Controls
SOC Report Review Checklist – Questions & Answers

What is the difference between a SOC 1, a SOC 2, and a SOC 3 report?
The SOC 1 report provides information about the controls at a service organization that may directly impact the University's financial statements.

The SOC 2 report provides information about the suitability of the design and controls at the service organization relevant to security, availability, processing integrity, confidentiality or privacy.

The SOC 3 report covers the same principals as a SOC 2 report, but does not include the detailed understanding of the design of controls and the tests performed by the service auditor. This report provides the auditor's opinion on whether the service organization maintains effective controls over its systems and is typically intended for users who do not require a more thorough report that includes a detailed description of the design of controls or tests performed by the service auditor.

Examples where you might need a SOC 1 report

- Maintenance accounting software
- Trust department of banks and insurance companies
- Custodian for investment companies
- Mortgage services or depository institutions that service loans for others
- Other financial transaction financially significant systems

Examples where you might need a SOC 2 report

- Hosting and support services (e.g. cloud computing, IT infrastructure, data center management, logical security management)
- Sales force automation
- Health care claims management and processing
- Printing of customer statements where processing integrity and confidentiality are important
- Trust departments of banks and insurance companies
- Custodians for investment companies, storage and vaulting firms
- Mortgage services or depository institutions that service loans for others
- Other nonfinancial transaction processing or systems that are not financially significant

Examples where you might need a SOC 3 report are as the SOC 2 examples. Basically a SOC 3 report is a watered down version of the SOC 2 report. The SOC 3 report is generally made publically available to users (e.g. posted on the service provider's website). If we do not have an existing relationship with a vendor (i.e. they are a potential new vendor) they may not provide SIU with a copy of their SOC 2 report which provides details of their design controls. Instead, they may have a SOC 3 that could be reviewed for purposes of determining if SIU is comfortable contracting with the vendor.

What is the difference between a Type 1 and Type 2 report?

There are two *types* of SOC 1 and two *types* of SOC 2 reports.

> Type 1 reports provide an opinion as to whether the service organization's description "fairly presents" the system that was designed and implemented, and whether the controls were suitably designed to meet the criteria at a particular point in time.
>
> Type 2 reports include the same information as a Type 1 report and they also include an opinion as to whether the controls operated effectively during the specified period of time and whether the service organization is in compliance with the commitments in its statement of privacy practices, if the SOC report covers privacy.

Because the auditor's opinion in a Type 1 report is limited, a Type 2 report is generally preferable.

How do I review a SOC report and what am I looking for?

Complete the *SOC Report Review Checklist*. Your review will include three basic steps.

- Determine whether the report covers the services being contracted for.
- Review the SOC report to see if there are Complementary User Entity Controls (CUEC) and, if applicable, ensure that your department has implemented the recommended controls.
- If the SOC report indicates that the service provider uses subservice organization, indicate if a SOC report for the subservice organization was reviewed or if other compensating controls are considered to be sufficient.
- Conclude regarding whether it is appropriate to continue with a contractual relationship with the provider.

What are Complementary User Entity Controls (CUEC)?

CUEC's are controls that the service provide assumes you, as the client, will implement to complete the security. These CUEC's are outlined in the Scope section of the SOC report. If you do not have the CUEC's in place, you may not be able to rely upon the opinion in the SOC report.

What if the service provider or sub-service provider does not have a SOC report?

If the service provider or subservice organization do not have a SOC report prepared, the department should:

- Determine if compensating controls are in place, determine if those compensating controls provide sufficient level of comfort, document the compensating controls and justification for reliance,
- Discuss the need for assurance that strong internal controls are in place and encourage the service provider or subservice organization to engage a firm to conduct a SOC review prior to engaging the service provider, or
- Consider using a different service provider

Can I save a copy of the SOC report electronically for my records?

SOC reports often contain sensitive information about the service provider's business operations. In many cases, the service provider will require acceptance of a Non-Disclosure Agreement in order to access the SOC report. Given the sensitive nature of these reports, it is recommended that the full report not be stored electronically. It may be acceptable to save the opinion page and the list of compensating user entity controls for documentation purposes, but check with your service provider.

Can I share the SOC report with others?

The SOC report often contains sensitive information about the service provider's business operations. In many cases, the service provider will require acceptance of a Non-Disclosure Agreement in order to access the SOC report. As a general rule, the SOC report should not be shared with anyone without the consent of the service provider, other than University personnel who have a need to know.