

<b>Financial Process:</b>	<b>Service Organizations SOC Reports</b>	<b>Issue Date:</b>	<b>February 2019</b>
		<b>Number:</b>	<b>BP - 12.00</b>
<b>Topic:</b>	<b>Internal Control - Best Practices</b>	<b>Revision Date:</b>	<b>N/A</b>
<b>Applicable:</b>	<b>All State Departments</b>	<b>Page:</b>	<b>1 of 6</b>

State of Vermont  
Department of Finance and Management

---

Objective

Departments shall devise techniques and procedures to be aware of the financial and operational statuses of the Service Organizations they are contracting with and be informed annually of their Service Organization Control (SOC) reporting. Departments are responsible for collecting and reviewing their Service Organizations' SOC reports annually.

Risks

- ✓ Business risks from Service Organizations
- ✓ Undetected errors and irregularities from Service Organizations
- ✓ Weaknesses in internal control associated with Service Organizations

Definition

SOC for Service Organizations reports are designed to help Departments that utilize service organizations for services, gain trust and confidence in the service performed, and controls related to the services through a SOC report by an independent Certified Public Accountant (CPA). Each type of SOC for Service Organization report is designed to help service organizations meet specific user needs:

- ✚ **SOC 1 - SOC for Service Organization: Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting (ICFR)**

These reports, prepared in accordance with attestation standard AT-C Section 320, "Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting", established by the American Institute of Certified Public Accountants (AICPA). These reports are specifically intended to meet the needs of entities that use service organizations (user entities) and the CPAs that audit the user entities' financial statements (user auditors), in evaluating the effect of the controls at the service organization on the user entities' financial statements.


There are two types of reports for these engagements:

- ✓ **Type 1** – report on the fairness of the presentation of management's description of the service organization's system and the suitability of the **design of the controls** to achieve the related control objectives included in the description **as of a specified date**.

<b>Financial Process:</b>	<b>Service Organizations SOC Reports</b>	<b>Issue Date:</b>	<b>February 2019</b>
		<b>Number:</b>	<b>BP - 12.00</b>
<b>Topic:</b>	<b>Internal Control - Best Practices</b>	<b>Revision Date:</b>	<b>N/A</b>
<b>Applicable:</b>	<b>All State Departments</b>	<b>Page:</b>	<b>2 of 6</b>

- ✓ **Type 2** - report on the fairness of the presentation of management's description of the service organization's system and the suitability of the **design and operating effectiveness of the controls** to achieve the related control objectives included in the description **throughout a specified period**.

Use of these reports are restricted to the management of the service organization, user entities, and user auditors.

 **SOC 2 - SOC for Service Organizations: Trust Services Criteria, Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy**

These reports are intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems. These reports can play an important role in:

- ✓ Oversight of the organization
- ✓ Vendor management programs
- ✓ Internal corporate governance and risk management processes
- ✓ Regulatory oversight

There are two types of reports for these engagements and they are similar to the SOC 1 reporting requirements. See definition type above.

 **SOC 3 - SOC for Service Organizations: Trust Services Criteria for General Use Report**

These reports are designed to meet the needs of users who need assurance about the controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy, but do not have the need for or the knowledge necessary to make effective use of a SOC 2 Report. Because they are general use reports, SOC 3 reports can be freely distributed.

<b>Financial Process:</b> Service Organizations SOC Reports	<b>Issue Date:</b> February 2019 <b>Number:</b> BP - 12.00
<b>Topic:</b> Internal Control - Best Practices	<b>Revision Date:</b> N/A
<b>Applicable:</b> All State Departments	<b>Page:</b> 3 of 6

Which SOC Report to request & review by the Departments?

<b>Key Questions to external Service Organizations (SO)?</b>	<b>SO's Response</b>	<b>Report Requested by Departments</b>	<b>What SOC does the Departments need to review? Is an <b>Action Plan</b> needed?</b>
Will the report be used by your customers and their auditors to <i>plan and perform an audit or integrated audit of your customer's financial statements?</i>	YES	<b>SOC 1 Report</b> ----- Type 1 or Type 2 (a)(c)	Departments <b>MUST</b> obtain and review its Service Organization's annual SOC 1 report, including examining the 1. The Overall <b>Audit Opinion</b> . 2. <b>Management's assertions</b> . 3. The <b>scope</b> of the report covers the services you are receiving. 4. The <b>time period</b> covered by the report. 5. The Types of <b>Exceptions Noted</b> . 6. Any related <b>Complementary User Controls</b> that should be <b>implemented and evaluated</b> . 7. Any <b>Sub-Service Providers</b> used. 8. Action Plan – <b>See note (b)</b> .
Do your customers have the need for and ability to <i>understand the details of the processing and controls at a service organization, the tests performed by the service auditor and results of those tests?</i>	YES	SOC 2 Report	Departments <b>May, If Necessary</b> , obtain and review its Service Organization's annual SOC 2 report, including examining the: 1. The Overall <b>Audit Opinion</b> . 2. <b>Management's assertions</b> . 3. The <b>scope</b> of the report covers the services you are receiving. 4. The <b>time period</b> covered by the report. 5. The Types of <b>Exceptions Noted</b> . 6. Any related <b>Complementary User Controls</b> that should be <b>implemented and evaluated</b> . 7. Any <b>Sub-Service Providers</b> used. 8. Action Plan – See note (b).
Will the report be used by your customers or stakeholders to <i>gain confidence and place trust in a service organization's systems?</i>	YES	SOC 2 Report Type 1 or Type 2  Or SOC 3 Report	Departments <b>May, If Necessary</b> , obtain and review its Service Organization's annual SOC 2 report, including examining the: 1. The Overall <b>Audit Opinion</b> . 2. <b>Management's assertions</b> . 3. The <b>scope</b> of the report covers the services you are receiving. 4. The <b>time period</b> covered by the report. 5. The Types of <b>Exceptions Noted</b> . 6. Any related <b>Complementary User Controls</b> that should be <b>implemented and evaluated</b> . 7. Any <b>Sub-Service Providers</b> used. 8. Action Plan – See note (b).

<b>Financial Process:</b>	<b>Service Organizations SOC Reports</b>	<b>Issue Date:</b>	<b>February 2019</b>
		<b>Number:</b>	<b>BP - 12.00</b>
<b>Topic:</b>	<b>Internal Control - Best Practices</b>	<b>Revision Date:</b>	<b>N/A</b>
<b>Applicable:</b>	<b>All State Departments</b>	<b>Page:</b>	<b>4 of 6</b>

**Notes:**

- a) Departments should **obtain and annually review** the SOC 1 Report, Type 2 from their service organization.
- b) Action Plan: Departments **must** obtain an action plan from the service organization for any deficiency or noncompliance included in the SOC for Service Organization report. Departments **must** document any procedures that are implemented to mitigate the service organization's deficiency.
- c) Departments should **proactively plan ahead** during the RFP process (during the finalist selection) to request that a SOC 1, Type 2 report be supplied annually, so as to defray any costs, prior to a contractual agreement being signed.

Best Practices Include

- ✓ Departments monitor annually their service organizations SOC 1 report. [\[Monitoring Activities\]](#)
- ✓ Departments review their service organization SOC 1 report for overall audit opinions, exceptions, and recommended user controls, and document their review. [\[Risk Assessment\]](#)
- ✓ Departments retain their service organizations SOC 1 report and documentation of that review for internal SAIC audit reviews and financial statement audits. [\[Information & Communication\]](#)
- ✓ Departments help to manage business risks, improve fiscal management, and safeguard the state's assets. [\[Control Activities\]](#)

SOC Report – Departments Review (Compliance Samples)

- ✚ **Unqualified Opinion** = Gold Star. Unqualified means controls are described in a fair and accurate manner and operate effectively. Simply, the controls abide by all of the standards. Typical language is as follows (SOC, Type II):

“In our opinion, in all material respects, based on the criteria described in the Company’s assertion in section II, the description fairly presents the System that was designed and implemented throughout the Period. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the Period and user entities applied the complementary user entity controls contemplated in the design of the Company’s controls throughout the Period. the controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable

<b>Financial Process:</b>	<b>Service Organizations SOC Reports</b>	<b>Issue Date:</b>	<b>February 2019</b>
		<b>Number:</b>	<b>BP - 12.00</b>
<b>Topic:</b>	<b>Internal Control - Best Practices</b>	<b>Revision Date:</b>	<b>N/A</b>
<b>Applicable:</b>	<b>All State Departments</b>	<b>Page:</b>	<b>5 of 6</b>

assurance that the control objectives stated in the description were achieved, operated effectively throughout the Period.”

[\[SOC - Audit Opinion Sample\]](#)

✚ **Audit Exceptions** can be intentional or unintentional, qualitative or quantitative, and include omissions. Auditors are required to make sure a service organization’s description is accurate and to include all design and operating deficiencies in the report—they no longer have discretion in determining whether or not to include exceptions.

There are three basic types of exceptions when it comes to SOC audits:

1. Misstatements: a misstatement is used to refer to an error or omission in the description of the service organization’s system or services.
2. Deficiency in the Design of a Control: a design deficiency is used when a control necessary to achieve the control objective or criteria is missing or an existing control is not properly designed, even if the control operates as designed, to achieve the control objective or criteria.
3. Deficiency in the Operating Effectiveness of a Control: an operating deficiency is when a properly designed control does not operate as designed or when the person performing the control does not possess the necessary authority or competence to perform the control effectively.

[\[SOC - Exceptions Noted Sample\]](#)

✚ **Complementary User Entity Controls (CUEC)** are controls that reside at the user entity level of a service organization. CUEC’s are controls that your Departments should have in place and operating effectively. Here are some samples:

- ✓ **Managed Service Provider (MSP) Environment Changes:** A user entity uses a managed IT service provider (service organization) to make changes to its environment, however, no changes are made to the service organization without explicit approval from the user entity. In this example, the service organization’s report would say that user entities must approve all changes prior to implementation.
- ✓ **Encrypted Financial Data:** A service organization works with banking institutions that send large amounts of data periodically to the service organization. A CUEC within the service organization’s report may say that user entities must send data in an encrypted manner using industry standard encryption or request that the service organization provide a secure transmission method.
- ✓ **Security Monitoring:** User entities must monitor and update their own antivirus definition updates and security patches unless the service is included within a contracted Statement of Work with the service organization. **Physical Access:** It is the responsibility of user entities to notify the service organization in the event that physical access needs to be added, modified, or revoked for a user entity’s employees.

<b>Financial Process:</b>	<b>Service Organizations SOC Reports</b>	<b>Issue Date:</b>	<b>February 2019</b>
		<b>Number:</b>	<b>BP - 12.00</b>
<b>Topic:</b>	<b>Internal Control - Best Practices</b>	<b>Revision Date:</b>	<b>N/A</b>
<b>Applicable:</b>	<b>All State Departments</b>	<b>Page:</b>	<b>6 of 6</b>

Contingency Plan: The service organization's contingency plan is applicable to its operations only. User entities are not covered by it and should develop their own contingency plan.

[\[SOC - Complementary User Control Sample\]](#)

BP # 12 SOC Report and Departments - SOC Checkoff List

<https://finance.vermont.gov/policies-and-procedures/internal-controls>

Notices

- ✓ These best practices are intended to support the internal control framework as presented in the [Internal Control Standards: A Guide for Managers](#).
- ✓ In consideration of these best practices, the objective should be on adherence and not on rationalizing ways and means for circumvention. Nothing in this document shall limit or supersede any applicable Federal or State laws, statutes, bulletins, or regulations.

Acknowledgment

- ✓ The State of Vermont, Department of Finance and Management would like to acknowledge the AICPA website for its publications of rules for SOC guidelines and CoNetrix for their model of a SOC check-off list.

