System and Organization Controls (SOC) report review template

**Reviewed by:** *Reviewer’s full name and title*

**Reviewed date:** *MM/DD/YYYY*

**Name of service organization:** *ABC Company*

**System(s) being covered:** *Example processing system*

**Type of Report:** *SOC 1 Type 1, SOC 2 Type 2, etc.*

**Coverage / Period:** *As of Sept. 30, 2023, Oct.1, 2022, to Sept. 30, 2023, etc.*

**Type of opinion:** *Unqualified, qualified*

**If qualified, basis for qualification:** *Basis of qualification and implications*

**Service auditor firm:** *Accounts & Accountants LLC*

**Independent service auditor’s report**

|  |  |  |
| --- | --- | --- |
| **Review area**  | **Y/N**  | **Comments (if any)**  |
| **Is the audit period appropriate?**  |   | *{A period of less than six months or a Type 1 report provides limited value since the controls are not tested for operating effectiveness. In addition, the timing of the SOC period end should be considered against your own fiscal year to determine if a gap exists and if further audit/vendor oversight procedures may be needed. Typically, the service organization will provide a bridge/gap letter to assert that the controls have not significantly changed and that there have been no significant control issues since the report was issued or to describe changes that have occurred. However, if the bridge/gap period is greater than 90 days, you should evaluate if a bridge letter is sufficient or if additional procedures are needed.}*  |
| **Does the scope provide adequate coverage for our business needs?**  |   | *{Verify that the right SOC report has been obtained. If not, then work with provider to obtain the correct report. If no report is available, then management should document how they gain comfort that the service being provided is adequate. (This is likely documented outside of this template and within your overarching vendor management assessment.)}*  |
| **Is the opinion stated?**  |   | *{Qualified/unqualified: Will be indicated by the “basis for qualified opinion” paragraph in the auditor's opinion letter, or in the opinion paragraph - a statement saying that "in all material respects" the bullet points are met.  Carefully review any opinion that begins with “Except for…”}*  |
| **Are the identified (if any) subservice organization(s) appropriate?**  |   | *{Refers to any cases where the service organization has in turn outsourced some of their control processes; will be mentioned in the opening paragraphs of the auditor's opinion as "service org XYZ uses company ABC to perform [list the activities]" type of language; will be mentioned as either carve out or inclusive. No mention of subservice organizations means that none are used (N/A).}*  |
| **Do subservice organization controls impact our operations? If yes, should we request a SOC report from them?**  |   | *{After reviewing the services performed by the subservice organization, if applicable, evaluate if the services impact your operations and how you will gain comfort of the controls at the subservice organization.  Consider if you should request and evaluate the SOC report of the subservice organization}*  |
| **Does the report include complementary user entity control considerations and/or user entity responsibilities? If yes, see below.**  |   | *{Complementary user entity control considerations are the specific controls user entities need to implement to complement the controls provided by the service organization. User entity responsibilities are the obligations and responsibilities of the user entity in relation to the use of services provided by the service organization.}*  |

**Complementary user entity control considerations (CUEC)**

|  |  |  |
| --- | --- | --- |
| **Description**  | **Does this apply to our organization? Y/N**  | **Our processes or controls in place to address?**  |
| *{Taken directly from the SOC report}*  |   | *{Describe the control activity in place at our organization that addresses the listed CUEC.}*  |

**Examination results**

|  |  |  |
| --- | --- | --- |
| **Control objective or criteria**  | **Control activity**  | **Testing results and our conclusion**  |
| *{Taken directly from the SOC report}*  | *{Taken directly from the SOC report}*  | *{Testing results taken directly from the SOC report}* *and* *{Our analysis and conclusion of the impact of any exceptions identified (e.g., did the SOC report sufficiently addresses our vendor control monitoring needs and if not, what actions will be taken with the service organization in a specific timeline and who’s in charge)}*  |