SOC 2® Report Review:

Note: This form is intended to be used as a tool in the evaluation of a vendor's SOC 2 report or, for organizations who rely on a third-party risk management (TPRM) solution, to ensure the TPRM solution is capturing all pertinent data.

Overview/general

System name	*System name*
Report period ("as of" for type 1, period for type 2) **Is there a gap since the last period?**	*XX/XX/XXXX type 1* *XX/XX/XXX – XX/XX/XXXX type 2*
Trust services categories in scope	*Security, Availability, Confidentiality, Processing Integrity, Privacy, Additional Criteria (or HIPAA, etc.):*
Type of opinion (See Appendix 4)	*Unmodified/Qualified/Adverse/Disclaimer*
If the opinion is anything other than "Unmodified," what is the reason and its impact on our use of the system/service?	

Independent service auditor (CPA firm) and report information

CPA firm name **If a recurring provider, has there been a change in independent service auditors?**	*Firm name*
CPA firm state	
Date of audit report (from CPA firm)	*XX/XX/XXXX*
CPA firm license current? **What is the current peer review result?**	*https://peerreview.aicpa.org/index.html* *Note: Only a licensed CPA firm can issue a valid SOC 2 report*

Procedures

During our review of the **SOC 2** report, management considered the following items:

Does the SOC 2 report cover the relevant systems, processes, and locations that we have outsourced to the vendor? (If no, get relevant SOC 2 report from service organization management.)	For example, enterprise cloud applications — Yes/no
How adequate are the governance-related controls?	

Are the trust services categories covered by the report sufficient to meet our needs? (See Appendix 5.)	Yes/no
Are the service commitments and system requirements identified in the system description sufficient to address our needs with the services we utilize?	Yes/no
If type 2: Does the period of the SOC 2 report cover sufficient period of time and is it recent enough to be useful for our evaluation?	Yes/no If no, is a bridge letter provided to cover the timing difference?
Are management-defined controls specific enough? Are they controls? Did control wording change significantly due to changing independent service auditors? **Do they have sufficient change controls?**	Yes/no
Do the controls listed in the report appear to be tailored to the specifics of the system being examined? ***For example, are the logical security controls tailored for the applications and infrastructure in scope as described in the system description and addressing the risk of the access expected by a user entity?***	Yes/no If no, the TPRM team may need to perform additional evaluations to determine whether the SOC 2 report can be relied upon for its purposes.
Did the independent service auditor apply appropriate procedures to test the operating effectiveness of controls? ***Note: Inquiry-based procedures are not appropriate unless supported by additional inspection, observation, or reperformance procedures.***	Yes/no If no, the TPRM team may need to perform additional procedures to evaluate the operating effectiveness of the inappropriately tested controls.
Were exceptions noted in tests of controls, and if so, have we evaluated their impact on the services provided to us by the vendor?	Yes/no If yes, refer to Appendix 1.
Does the SOC 2 report disclose any system events or incidents within the system description that may affect the services provided to us?	Yes/no
Does the SOC 2 report note any significant changes to the system during the audit period?	Yes/no
Does the SOC 2 report identify controls that we, as the user entity, need to implement for the service commitments and system requirements to be met (complementary user entity controls or CUECs), and if so, have we evaluated whether such controls have been implemented within our organization?	Yes/no If yes, refer to Appendix 2.

Does the SOC 2 report identify any activities that we, as the user entity, need to perform to derive value from the services (user entity responsibilities), and if so, have we evaluated whether such activities have been implemented within our organization?	Yes/no If yes, refer to Appendix 3.
Does the SOC 2 report identify subservice organizations that perform services on behalf of the vendor and that have been carved out (excluded) from the scope of the SOC 2 report? If so, have we evaluated whether service organization management's monitoring of these subservice organizations (as described in the system description) is adequate for our purposes? **Note: If it is determined that management's monitoring function is inadequate, it may be necessary to obtain a SOC or equivalent report for each relevant subservice organization and complete a separate review.**	Yes/no
Does the description describe tools used to prepare the SOC 2 report and ownership/hosting of those tools? **If yes, is the tool considered a subservice organization?**	Yes/no Yes/no
Has the auditor included an "emphasis-of matter" or "other matter" paragraph within the auditor's report section to call attention to any pertinent information? If so, have we evaluated the impact of this information?	Yes/no
Other comments stemming from a detailed review of the report	
Are there any publicly known incidents/outages/leadership issues/changes of ownership of the service organization or any of its subservice organizations? What is the impact on our security and availability needs?	Yes/no
Did our SOC 2 report review result in anything that is contradictory to our relationship or perspectives of the vendor service organization and the services that we rely upon?	Yes/no If yes, summarize and determine if more consideration and discussion is needed with management or oversight personnel.

Follow-up actions

In the space below, document any follow-up actions or conversations held with the vendor that were deemed necessary before forming a conclusion on the continued use of the vendor.

Conclusion

Based on the preceding evaluation, management concludes that:

Criteria	Initial
The continued use of this vendor is approved until the next review cycle.	
Evaluation completed by:	
Print name/title	
Signature	
Date	

Evaluation reviewed by:

Print name / Title

Signature

Date

Appendix 1 — Examination results

We evaluated the following exceptions/deviations identified by the independent service auditor according to the test results within section 4 of the SOC report.

Control activity	Exception noted	Affected criteria	Service organization's response (if included) and our evaluation
Example: User access is removed within twenty-four (24) hours of termination.	Example: For one (1) of twenty-five (25) user terminations selected for testing, the user's access was not removed from the system within 24 hours.	Example: CC6.2, CC6.3	Example: Management determined the user's access was removed within forty-eight (48) hours of termination. Management reviewed access logs during the 48 hours after the user's termination and determined that the user did not log in or access the system after termination. Because management has enhanced the control and the control does not have a material impact on system access, we feel there were sufficient mitigation controls in place (most notably the controls related to access reviews), and we do not feel this risk affects the XYZ Company control environment. (Note: Other important factors to consider include: 1. Did the exception language provide enough detail to understand the situation? 2. How critical is the affected control to the service provided by the service organization? 3. Did the finding lead to a larger security incident? 4. Did the affected control relate directly to a risk in our risk assessment? 5. Was management's response detailed enough to understand the current disposition of the control and future plans to reduce risk? 6. Was management's response in Section IV as audited or unaudited? 7. Was the same exception noted in the prior year's reports, if available?)

Appendix 2 — Complementary user entity control considerations (not common)

Within SOC 2 reporting, an end user or customer is defined as a user entity. Complementary user entity controls (CUECs) are controls that the service organization expects the user entities to implement to enable the service organization to meet its service commitments and/or systems requirements. Put differently, without a user entity implementing the CUECs noted in the report, the system and its controls may not be sufficient or complete or may be compromised. CUECs should be uncommon in SOC 2 reports because, in most cases, a system is designed in such a way that the service organization can achieve its service commitments and system requirements without reliance on its user entities to perform controls. The following CUEC(s) map to our internal controls and internal controls testing:

CUEC noted by the service org	Related trust services criteria	Internal control ID or description	Control tested?
Example: Customers should ensure appropriate physical access restrictions are in place to safeguard service organization servers co-located in customer data centers.	Example: CC6.4	Example: We have access restrictions preventing unauthorized individuals from accessing our on-premises data center, including the use of cameras, fob/PIN locks, and visitor escort provisions.	Example: Physical access controls are included in our annual internal audit program. No material findings noted from most recent testing.

Appendix 3 — User entity responsibilities

User entity responsibilities are activities that must be performed by user entities to derive the intended benefits of using the service organization's system. They are similar in concept to CUECs but are not required by the service organization to meet its service commitments and/or service requirements.

The following user entity responsibilities are outlined:

Subservice user identity responsibilities	Related control area	Internal control ID or description	Control tested?
Example: Customers should establish, monitor, and maintain controls to ensure appropriate access to applications, the system, or information on <<IaaS Cloud>>. Customers should assign an individual to perform user access administration responsibilities.	Example: Access	Example: Access is restricted to authorized users with an established business need. This is documented in access requests forms. Access is approved by managers, is reviewed quarterly, and is disabled within 24 hours of termination or loss of need.	Example: Access provisioning, review, and termination controls are included in our annual internal audit program. No material findings noted from most recent testing.

Appendix 4 — Types of auditor's opinions

Based on the results of the audit procedures or attempted auditor procedures, the independent service auditor will issue one of the following types of opinions:

1. Unmodified
2. Qualified
3. Adverse
4. Disclaimer

The following information is intended to help report users identify and interpret the specific opinion types. The opinion will be found in the auditor's report section of the overall SOC 2 report and is typically labeled "opinion." Note that bold text is used for emphasis to point out differences between the types of opinions. Also note that the language used in the independent service auditor's opinion may vary slightly from what is presented below.

1. **Unmodified opinion (commonly seen)**

An unmodified opinion is the best result of a SOC examination and indicates that the independent service auditor did not note any material factors affecting the opinion. This does not necessarily mean that there were no exceptions noted, but only that the noted exceptions, if any, did not negatively affect the opinion.

Language used:

"In our opinion, in all material respects,

a. *the description of the system presents the system that was designed and implemented throughout the period in accordance with the description criteria;*
b. *the controls stated in the description were suitably designed throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria; and*
c. *the controls stated in the description operated effectively throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria."*

2. **Qualified Opinion (commonly seen)**

A qualified opinion indicates that the independent service auditor identified material factors affecting the opinion. This may stem from misstatements in the system description or from control design or operating effectiveness exceptions. It may also stem from a lack of evidence to support control design or operation (this would be called a scope limitation). However, to warrant a qualified opinion rather than an adverse or disclaimed opinion, which are described below, the independent service auditor would have determined that the factors noted were limited in scope rather than pervasive throughout the service organization's system.

Language used:

"In our opinion, ***except for the effects of the matters giving rise to the modification****, in all material respects,*

a. *the description of the system presents the system that was designed and implemented throughout the period in accordance with the description criteria;*
b. *the controls stated in the description were suitably designed throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria; and*

c. *the controls stated in the description operated effectively throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria."*

Note: If the qualified opinion was the result of a scope limitation, the bold text above would read: "except for the **possible effect of** the matter giving rise to the modification …" A scope limitation means that the auditor was unable to perform a planned test. This is often the result of management's inability to find and provide the required evidence.

In addition to the qualitied opinion itself, the auditors' report will also include a separate paragraph describing the reason for the qualification. The opinion paragraph will generally refer to this paragraph. It is important to read and understand why the opinion was modified and to consider the impact of the reason for the modification on your needs as a user entity.

3. **Adverse opinion (rarely seen)**

An adverse opinion indicates the independent service auditor has identified factors affecting the opinion that were both material and pervasive. The factors may be related to misstatements in the system description or deficiencies in control design or operating effectiveness. Adverse opinions are indicative of significant issues within the service organization's system, and users should use this information accordingly for their decision-making.

Language used:

*"In our opinion, **because of the significance** of the matter(s) referred to in the preceding paragraph, in all material respects,*

a. *the description of the system **does not present** the system that was designed and implemented throughout the period in accordance with the description criteria;*

b. *the controls stated in the description **were not suitably designed** throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria; and*

c. *the controls stated in the description **did not operate effectively** throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria."*

4. **Disclaimed opinion (rarely seen)**

If unable to obtain a substantial portion of the evidence required to evaluate the service organization's system, the independent service auditor will generally withdraw from the examination and not provide an auditor's report. However, in some limited circumstances when withdrawal is not possible, the independent service auditor will issue a report disclaiming an opinion. Disclaimed opinions are indicative of missing information for the auditor, and users should use this information accordingly for their decision-making.

Language used:

The first sentence of the auditor's report will state:

"We were engaged to examine …" rather than the typical "*We have examined …."*

Also, the opinion language shown in the prior examples will be replaced by a paragraph stating:

"Because of the significance of the matter giving rise to the modification, the service auditor has been unable to obtain sufficient appropriate evidence to provide a basis for an opinion, and accordingly, the service auditor does not express an opinion."

Appendix 5 — SOC 2 categories

SOC 2 reports may include any combination of the following categories. The scoping is determined by management and should reflect the nature of the services provided.

Security — Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

Availability — Information and systems are available for operation and used to meet the entity's objectives.

Processing integrity — System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

Confidentiality — Information designated as confidential is protected to meet the entity's objectives.

Privacy — Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.

The in-scope trust services categories can typically be found in the first paragraph of the auditor's report and management's assertion using the following language:

"…. service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA *Trust Services Criteria*."

Note: The preceding language in *italics* is a reference to the TSP section 100 title and is not referring to the in scope categories. The in-scope categories are listed prior to the TSP reference and are underlined here for emphasis.