SOC 2 Review Template

Contents

Disclaimer:

This template is provided as a general guide for reviewing SOC 2 reports. Your company's third-party assurance requirements may have separate or additional requirements beyond what is described here. If you encounter any content or recommendations within the template, please let us know at angelika@rendercompliance.com.

SOC 2 Review Template Basic

Company Details (the company that the SOC report is about)	
1.Company Legal Name	
2.Company Location	
3.What services of the company we are using	
4.Our Data types processed or stored by company	
Audit Information	
5.Type of report	
6.System Name	
7.Trust Services Categories	
8.Auditor's name	
9.Auditor's opinion	
10.Date of Auditor's opinion	
11.Examination Period	
12.Exceptions/ Deviations noted by Auditor (if any), Management Response	
13.Complementary Subservice Organizations	
14.Complementary Subservice Organizations Controls (CSOCs)	
15.Complementary User Entity Controls (CUECs)	
16.User Entity Responsibilities (UERs)	

Detailed information	
17.Section 3 – System description, key components (tailored to the specific services the third-party vendor is providing to your organization)	
Conclusion and Approval	
18.Conclusion	
19.Preparer, Date	
20.Reviewer, Date	

SOC 2 Review Template Advanced

Additional Assurance in specified areas	
This section is optional, complete this section as needed to gain additional assurance in the specified functional areas.	
Business Continuity: The Auditor has confirmed through testing that Business Continuity and Disaster Recovery have been documented and are in place. Disaster recovery testing is performed annually.	Page:
Incident Response: Incident detection and reporting protocols are in place. Response programs and protocols define actions for when unauthorized access to information systems or facilities is suspected or detected to include incident response and remediation.	Page:
Human Resources Policies: Values and behavioral standards are communicated to personnel through policy statements and code of conduct. Employee sanction statements are documented within the code of conduct to communicate consequences for policy and code violations. Background check is performed upon hire for all employees.	Page:
Anonymous Reporting/Ethics Reporting/Whistleblower Hotline: A whistleblower process is in place to facilitate reporting of unethical behaviors and fraudulent activities that become known to an employee.	Page:
Risk Assessment and Mitigation Controls: Formal procedures are implemented to identify and assess the likelihood and impact of reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of information or systems. Controls exists to remediate identified risks and vulnerabilities.	Page:

Logical Access Authentication: Logical access is restricted to appropriate personnel and authenticated through password parameters or other protocols to authenticate users.	Page:
Logical Access Periodic Review: Formal procedures are implemented to review logical access permissions and appropriateness.	Page:
Onboarding/ Termination Protocols: Onboarding and termination protocols for personnel includes management provisioning/removal of logical/physical access permissions.	Page:
Data Inventory: An information management program identifies, classifies, and tracks data within the organization.	Page:
Encryption at Rest or During Storage: Confidential electronic information is encrypted while in storage or at rest.	Page:
Encryption During Transmissions: Confidential electronic information is encrypted while in transit between networks or systems.	Page:
Change Management Policy and Controls: A change management policy defines protocols for the approval and implementation of operational changes within the organization.	Page:
Firewalls/IPS/IDS/SIEM: The Company has prevention and response systems and controls to prevent and/or detect actual and attempted attacks on, or intrusions into, information systems.	Page:
Network Testing: Penetration tests, vulnerability scans, and/or other network security testing are performed to validate system integrity.	Page:
Data Backup/Replication: Data is backed up, replicated, or mirrored to an alternate system and/or location.	Page:
Third-Party Monitoring: Due diligence for a third-party provider is performed during onboarding and annually thereafter.	Page:

Guide – Where Do I Find That Information?

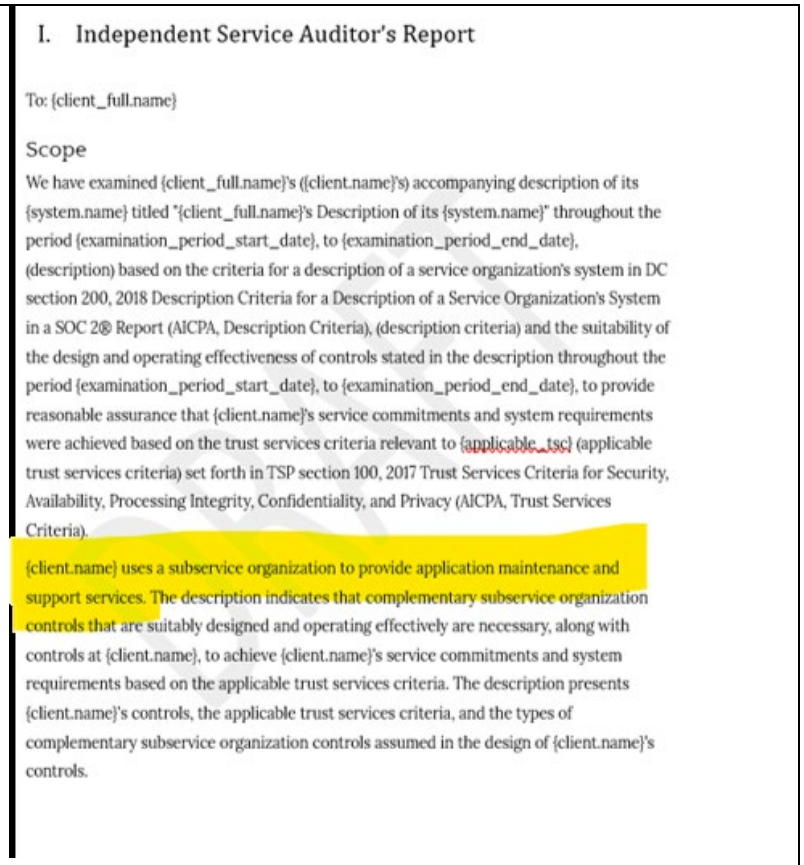
Asked for	Where to find within a report	Screenshot where to find
1.Company Legal Name	On the Title Page of the report Or In Section 1 of the report, first sentence	
2.Company Location	Most likely not within the report. Search for Headquarters within the company website, or on a Master Service Agreement (MSA). Important to check due to regulatory compliance, jurisdictional risk, data sovereignty, political and economic stability, and business continuity planning.	n/a, not within SOC report.
3.What services of the company we are using	Check within the Statement of Work (SOW) or Master Service Agreement (MSA) Very important to check so you can ensure that product/services you are using from a Company actually are covered within provided SOC report.	n/a not within SOC report.
4.Our Data types processed or stored by company	Check within the Statement of Work (SOW) or Master Service Agreement (MSA). Very important to ensure that you understand what kind of data type will be processed or stored by the subservice provider.	n/a not within SOC report.

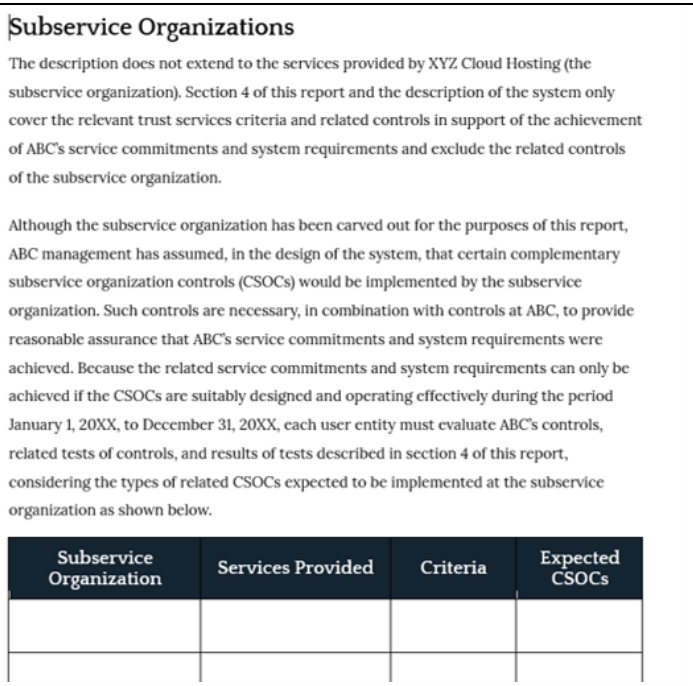
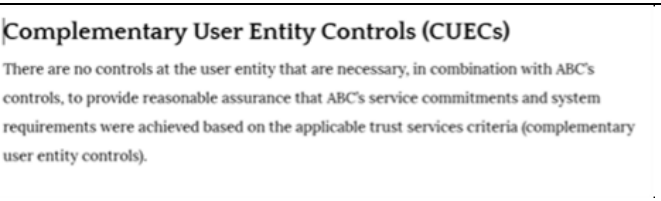
5.Type of a report	On the Title Page of the report, you can find the Type of report (SOC 1 or SOC 2, Type 1 or Type 2). If it is Type 2, it will have language throughout about “examination period”. Type 1 will have the language "as of {date}”	
6. System Name	In Section 1 of the report, first sentence Or (more information) in Section 3 of the report, first paragraph	I. Independent Service Auditor’s Report To: {client_full.name} Scope We have examined {client_full.name}’s ({client.name}’s) accompanying description of its {system.name} titled “{client_full.name}’s Description of its {system.name}” throughout the
7. Trust Services Categories	In Section 1, under Scope - red circle in screenshot, don’t get confused by the boilerplate language listing all possible criteria (red x). There are 5 categories of criteria possible for a SOC 2, including Security, Availability, Confidentiality, Processing Integrity, and Privacy.	I. Independent Service Auditor’s Report To: {client_full.name} Scope We have examined {client_full.name}’s ({client.name}’s) accompanying description of its {system.name} titled “{client_full.name}’s Description of its {system.name}” throughout the period {examination_period_start_date}, to {examination_period_end_date}, (description) based on the criteria for a description of a service organization’s system in DC section 200, 2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report (AICPA, Description Criteria), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period {examination_period_start_date}, to {examination_period_end_date}, to provide reasonable assurance that {client.name}’s service commitments and system requirements were achieved based on the trust services criteria relevant to {applicable_tsc} (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

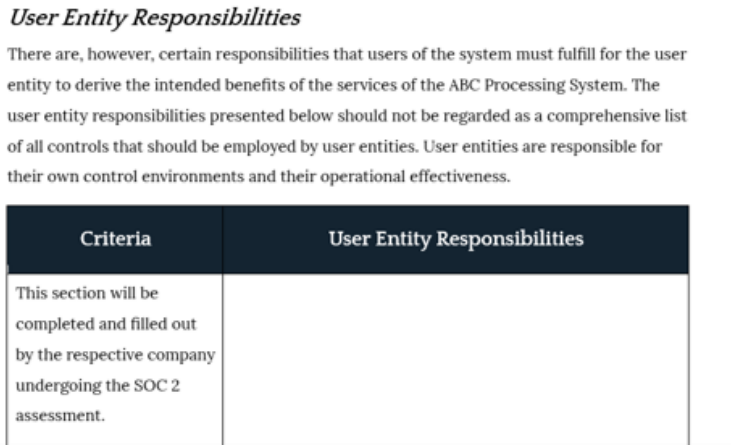
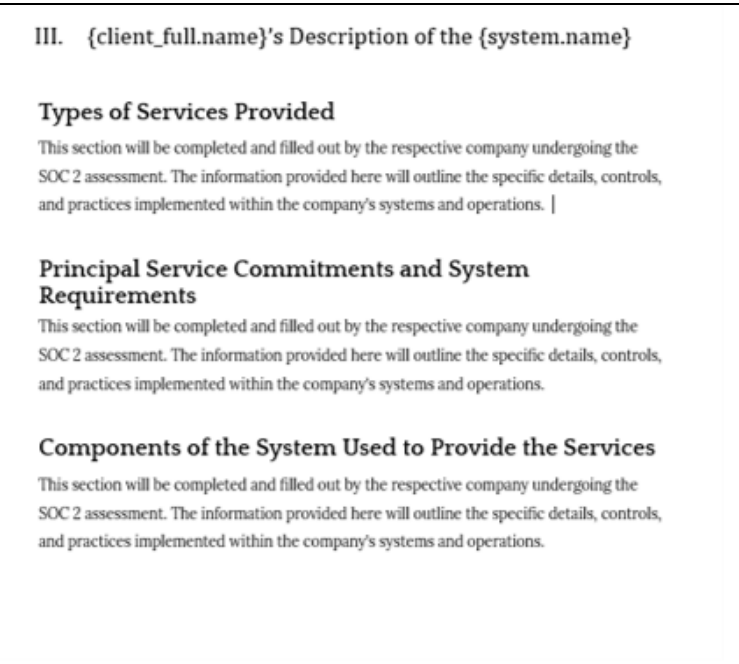
8.Auditor's name	In Section 1, on the end, there is the auditor's signature. Important to verify they have a current CPA firm license on CPA Verify - **https://app.cpaverify.org/search**	[Service auditor's signature] [City and state where the report is issued] [Date of the service auditor's report] II. Assertion of {client_full.name} Management
9.Auditor's opinion	In Section 1, Section called 'Opinion'. There might be four types of opinion issued by the Auditor: a. **Unqualified Opinion**, This is issued when the service auditor concludes that the description of the system is fairly presented, the controls are suitably designed, and, in the case of a Type 2 report, that the controls operated effectively throughout the specified period. How to Identify: you'll find language like: "The controls stated in the description were suitably designed ..." "The controls stated in the description operated effectively throughout the period ..." b. **Qualified Opinion**, This is issued when the service auditor concludes that, except for the effects of certain matters, the description of the system is fairly presented, the controls are suitably designed, and (in the case of a Type 2 report) that the controls operated effectively throughout the period.	Opinion In our opinion, in all material respects, a. the description presents {client.name}'s {system.name} that was designed and implemented throughout the period {examination_period_start_date}, to {examination_period_end_date}, in accordance with the description criteria. b. the controls stated in the description were suitably designed throughout the period {examination_period_start_date}, to {examination_period_end_date}, to provide reasonable assurance that {client.name}'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of {client.name}'s controls throughout that period. c. the controls stated in the description operated effectively throughout the period {examination_period_start_date}, to {examination_period_end_date}, to provide reasonable assurance that {client.name}'s service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of {client.name}'s controls operated effectively throughout that period.

	How to Identify: you'll find language like: "In our opinion, except for the effects of the matter(s) described in the Basis for Qualified Opinion paragraph..." c. **Adverse Opinion**, This is issued when the service auditor concludes that the description of the system is not fairly presented, the controls are not suitably designed, or (in the case of a Type 2 report) that the controls did not operate effectively. How to Identify: you'll find language like: "The controls stated in the description were NOT suitably designed [...]" "The controls stated in the description DID NOT operate effectively throughout the period." d. **Disclaimer of Opinion**: This is issued when the service auditor is unable to obtain sufficient appropriate evidence to provide a basis for an opinion.	
10.Date of Auditor's opinion	In Section 1, at the end there is a date of the service auditor's report. This date indicates when report was issued (different than examination period). This date helps determine whether the report is current and relevant to your assessment, and if it was issued within a reasonable time from the end of examination period. It can help you assess whether there was a delay in issuing the report, which could raise concerns about the accuracy or completeness of the findings.	[Service auditor's signature] [City and state where the report is issued] [Date of the service auditor's report] II. Assertion of {client_full.name} Management

11.Examination Period	In Section 1, under Scope Or Title page Examination Period refers to the specific timeframe during which the service organization's controls were assessed by the auditor.	I. Independent Service Auditor's Report To: {client_full.name} Scope We have examined {client_full.name}'s ({client.name}'s) accompanying description of its {system.name} titled "{client_full.name}'s Description of its {system.name}" throughout the period {examination_period_start_date}, to {examination_period_end_date},
12.Exception noted by Auditor	In Section V (Other Information) – look for a table of exceptions. Not all audit firms include it here. Or In Section IV – scroll through the Auditor's Test of Controls table and review the Results of Testing column. If there are exceptions, it will say "Exception noted," "Deviation noted," or provide a description of the issues identified, as opposed to the standard "No exceptions noted." If there are exceptions, review these to determine if your business is relying on any of those controls with issues, and if additional work may be needed.	V. Other Information Provided by {client_full.name} That Is Not Covered by the Service Auditor's Report Management's Response to Identified Testing Exceptions

13.Complementary Subservice Organization	If applicable, located in Section 1, under Scope, paragraph 2. Or In Section 3, under Subservice Organizations section, toward the end. Determine whether any subservice organizations are “carved out” of the report’s scope and assess how this impacts the level of assurance you receive from the report. Alternatively, check if any subservice organizations are marked as "Inclusive." If the CSOCs are "carved out," they are EXCLUDED from the scope of the main service organization's report (the company that the SOC report is about). This means the reader does not receive any assurance over those controls. The reader must either obtain the subservice organization’s report independently, place blind trust in the subservice organization, or rely on the main service organization’s vendor due diligence controls to ensure comfort.	 I. Independent Service Auditor’s Report To: {client_full.name} Scope We have examined {client_full.name}’s ({client.name}’s) accompanying description of its {system.name} titled "{client_full.name}’s Description of its {system.name}" throughout the period {examination_period_start_date}, to {examination_period_end_date}, (description) based on the criteria for a description of a service organization’s system in DC section 200, 2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report (AICPA, Description Criteria), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period {examination_period_start_date}, to {examination_period_end_date}, to provide reasonable assurance that {client.name}’s service commitments and system requirements were achieved based on the trust services criteria relevant to {applicable_tsc} (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). {client.name} uses a subservice organization to provide application maintenance and support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at {client.name}, to achieve {client.name}’s service commitments and system requirements based on the applicable trust services criteria. The description presents {client.name}’s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of {client.name}’s controls.

14.Complementary Subservice Organizations Controls (CSOCs)	If applicable, located in Section 3, toward the end there will be a CSOC listed, within a table (if any). CSOCs refer to controls that are implemented by subservice organizations (third-party vendors or service providers) that the main service organization (the company that the SOC report is about) relies on to meet its own control objectives. These controls are outside the direct control of the main service organization but are necessary for the main service organization's controls to be effective. What to do: **See page CSOCs**	 **Subservice Organizations** The description does not extend to the services provided by XYZ Cloud Hosting (the subservice organization). Section 4 of this report and the description of the system only cover the relevant trust services criteria and related controls in support of the achievement of ABC's service commitments and system requirements and exclude the related controls of the subservice organization. Although the subservice organization has been carved out for the purposes of this report, ABC management has assumed, in the design of the system, that certain complementary subservice organization controls (CSOCs) would be implemented by the subservice organization. Such controls are necessary, in combination with controls at ABC, to provide reasonable assurance that ABC's service commitments and system requirements were achieved. Because the related service commitments and system requirements can only be achieved if the CSOCs are suitably designed and operating effectively during the period January 1, 20XX, to December 31, 20XX, each user entity must evaluate ABC's controls, related tests of controls, and results of tests described in section 4 of this report, considering the types of related CSOCs expected to be implemented at the subservice organization as shown below. Subservice Organization | Services Provided | Criteria | Expected CSOCs
15.Complementary User Entity Controls (CUECS)	If applicable, located in Section 3, toward the end there will be CUECs listed, within a table (if any) some reports will not have it, e.g. example in column D. CUECs are controls that the service organization assumes will be implemented by its user entities (your organization) to meet the control objectives. These controls are outside the scope of the service organization's responsibility and need to be implemented by the user entity. What to do: **See page CUECs**	 **Complementary User Entity Controls (CUECs)** There are no controls at the user entity that are necessary, in combination with ABC's controls, to provide reasonable assurance that ABC's service commitments and system requirements were achieved based on the applicable trust services criteria (complementary user entity controls).

16.User Entity Responsibilities (UERS)	If applicable, located in Section 3, toward the end there will be a UER listed, within a table (if any) some reports will not have it. UERs are broader responsibilities that the user entity (your organization) must fulfill to effectively use the service provided. These responsibilities may include things like managing user accounts, maintaining the security of user endpoints, or configuring the service in a secure manner. What to do: **See page UERs**	 ***User Entity Responsibilities*** There are, however, certain responsibilities that users of the system must fulfill for the user entity to derive the intended benefits of the services of the ABC Processing System. The user entity responsibilities presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities. User entities are responsible for their own control environments and their operational effectiveness. **Criteria** / **User Entity Responsibilities** This section will be completed and filled out by the respective company undergoing the SOC 2 assessment.
17.Section 3 – System description, key components	Review the beginning of the System Description to ensure that the scope described aligns with your company's reliance on the company you are evaluating (e.g. make sure they didn't focus the scope of this report on a certain business unit and exclude the business unit that your company relies on).	 III. {client_full.name}'s Description of the {system.name} **Types of Services Provided** This section will be completed and filled out by the respective company undergoing the SOC 2 assessment. The information provided here will outline the specific details, controls, and practices implemented within the company's systems and operations. **Principal Service Commitments and System Requirements** This section will be completed and filled out by the respective company undergoing the SOC 2 assessment. The information provided here will outline the specific details, controls, and practices implemented within the company's systems and operations. **Components of the System Used to Provide the Services** This section will be completed and filled out by the respective company undergoing the SOC 2 assessment. The information provided here will outline the specific details, controls, and practices implemented within the company's systems and operations.

18.Conclusion	Conclude what you identified within the report such as "The report provides satisfactory assurance over our reliance of the core functional areas of information security for the company and examination date(s) noted. We noted the report was not sufficient to cover the following functional areas and we will follow up with the company regarding: ABC. The following items will be added to our risk register: XYZ."	n/a
19. Preparer, Date	Person who performed this SOC 2 Review	n/a
20. Reviewer, Date	Person who reviewed this SOC 2 Review	n/a

Business Continuity: The Auditor has confirmed through testing that Business Continuity and Disaster Recovery have been documented and are in place. Disaster recovery testing is performed annually.	In Section 3 of a report, called - System Description or in Section 4, as a control statement. Use Search (CTR+F/ Command (⌘) + F)
Incident Response: Incident detection and reporting protocols are in place. Response programs and protocols define actions for when unauthorized access to information systems or facilities is suspected or detected to include incident response and remediation.	
Human Resources Policies: Values and behavioral standards are communicated to personnel through policy statements and code of conduct. Employee sanction statements are documented within the code of conduct to communicate consequences for policy and code violations. Background check is performed upon hire for all employees.	
Anonymous Reporting/Ethics Reporting/Whistleblower Hotline: A whistleblower process is in place to facilitate reporting of unethical behaviors and fraudulent activities that become known to an employee.	
Risk Assessment and Mitigation Controls: Formal procedures are implemented to identify and assess the likelihood and impact of reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of information or systems. Controls exists to remediate identified risks and vulnerabilities.	

Logical Access Authentication: Logical access is authenticated through password parameters or other protocols to authenticate users.	
Logical Access Periodic Review: Formal procedures are implemented to review logical access permissions and appropriateness.	
Onboarding/ Termination Protocols: Onboarding and termination protocols for personnel includes management provisioning/removal of logical/physical access permissions.	
Data Inventory: An information management program identifies, classifies, and tracks data within the organization.	
Encryption at Rest or During Storage: Confidential electronic information is encrypted while in storage or at rest.	
Encryption During Transmissions: Confidential electronic information is encrypted while in transit between networks or systems.	
Change Management Policy and Controls: A change management policy defines protocols for the approval and implementation of operational changes within the organization.	
Firewalls/IPS/IDS/SIEM: The Company has prevention and response systems and controls to prevent and/or detect actual and attempted attacks on, or intrusions into, information systems.	
Network Testing: Penetration tests, vulnerability scans, and/or other network security testing are performed to validate system integrity.	
Data Backup/Replication: Data is backed up, replicated, or mirrored to an alternate system and/or location.	
Third-Party Monitoring: Due diligence for a third-party provider is performed during onboarding and annually thereafter.	

Complementary User Entity Controls (CUECs)

Why is it important: CUECs are controls that the service organization assumes will be implemented by its user entities (your organization) to meet the control objectives. These controls are outside the scope of the service organization's responsibility and need to be implemented by the user entity.

The effectiveness of some of the service organization's controls depends on the user entity (your organization) implementing certain controls on its end. For example, if the service provider secures its platform but the user doesn't implement strong access controls, the security of the data could be compromised.

List the CUECs in the left column and map Control Activities that your organization has in place in the right column.

Complementary User Entity Controls (CUECs)	Control Activity

User Entity Responsibilities (UERs)

Why is it important: UERs are broader responsibilities that the user entity (your organization) must fulfill to effectively use the service provided. These responsibilities may include things like managing user accounts, maintaining the security of user endpoints, or configuring the service in a secure manner.

UERs are crucial for ensuring that the service you are using operates securely and effectively. Without fulfilling these responsibilities, you may expose your organization to risks that could otherwise be mitigated.

List the UERs in the left column and map Control Activities that your organization has in place in the right column.

Complementary User Responsibilities (UERs)	Control Activity

Complementary Subservice Organizations Controls (CSOCs)

Why is it important: CSOCs refer to controls that are implemented by subservice organizations (third-party vendors or service providers) that the main service organization (the company that the SOC report is about) relies on to meet its own control objectives. These controls are outside the direct control of the main service organization but are necessary for the main service organization's controls to be effective.

Many organizations rely on third-party subservice organizations for critical functions (e.g., cloud hosting, payment processing). The effectiveness of the main service organization's controls often depends on the subservice organization's controls. If the subservice organization's controls fail, it could impact the main service organization's ability to meet its control objectives.

Subservice Organization	Control Activity	Do we Place Critical reliance on this control?