Vendor vs. Service Provider

For state agencies (agency or agencies) that have made the decision to contract with a third-party organization for some or all functions associated with service delivery, it is important for the agency to distinguish whether the organization is a "vendor" or a "service organization". An important criteria in determining whether the third-party organization is a "vendor" or a "service organization" is determining whether the service provided by the third party is likely to be relevant to financial reporting and/or the protection of confidential information (as classified by the state agency or compliance requirements). If the third-party organization was deemed relevant to financial reporting and/or the protection of confidential information, the state agency would classify the third-party as a "service organization" for the purpose of the state agency's internal control environment.

To determine if the third-party organization is a vendor or a service organization, the agency should consider whether financial and/or confidential data, that is the responsibility of the agency, resides at a location outside the boundaries of the agency. In this instance the third-party organization would be considered a service organization, and the agency should evaluate the service organization's internal controls prior to entering into an agreement as part of the agency's due diligence process. Then the agency should review and evaluate the service organization's internal controls with the service organization and on an annual basis for the term of the agreement.

For third-party organizations that provide a service to the agency, but do not transfer confidential data outside of the agency's environment, the organization would be considered a vendor. In this instance, the agency should have a written agreement that includes verbiage related to the non-disclosure of data that is accessed by the vendor's employees within the agency's environment. In addition, the agency should evaluate that the vendor requires background checks on employees as a condition of employment and prior to accessing the agency's environment where confidential information resides.

For example, an agency that has an agreement with a third-party to provide remote storage of electronic data is identified as a service organization. Even though controls related to the storage of data does not directly relate to user entities' internal control over financial reporting, accessibility and/or recovery of financial data in electronic format is key to the agency's internal control environment.

Another example of a service organization is if the third-party organization is responsible for performing data backups, and monitoring the status of the backup, on application servers within **a hosted environment**. However, if the third-party schedules and monitors backups for "on premise" servers **within the agency's environment** the organization would be considered a vendor.

The following was extracted from the AICPA SOC 1 Guide as further examples of services provided by third-party and determination if the organization is a service organization or vendor:

Service Provided to the Agency By a Third-Party Organization	Service Provided Relevant to the Agency's Internal Control Over Financial Reporting	Vendor or Service Organization
Software development The agency outsources the development of its application changes to a third-party software development organization. This organization receives the authorized changes from the agency, develops the changes, and sends them back to the agency. The agency authorizes all changes to be developed, reviews the accuracy of the changes, performs all user acceptance testing, and approves all changes prior to implementing them in production.	**No** In this scenario the organization would be considered a vendor because the agency's controls alone are sufficient to satisfy internal control over financial reporting.	Vendor
Application hosting The third-party organization manages all of the application systems for the agency within the third-party's environment	**Yes** The service provided by the application hosting organization relates to the agency's internal control over financial reporting because controls within the application that are managed by the third-party organization are necessary for the agency's application controls to operate effectively.	**Service Organization**
Cloud-based data processing The agency operates [utilizes] its application at a cloud-based data processing agency. Although the agency implements certain controls over the functions performed by the cloud-based data processing entity, the agency's controls alone are not sufficient to enable the agency to achieve the related control objectives because it relies on the effectiveness of certain controls at the cloud-based data processing entity, specifically, the IT general controls.	**Yes** The services provided by the cloud-based data processing entity are relevant to the agency's internal control over financial reporting because controls at the data-processing entity are necessary for the agency's controls to operate effectively.	**Service Organization**
Pharmacy claims processing This organization processes pharmacy claims for a medical claims processing service organization. Pharmacy claims are a subset of all the claims the medical claims processing service organization	**Yes** The processing performed by the pharmacy claims processor is relevant to the internal control over financial reporting of the agency that submits pharmacy	**Service Organization**

receives. The information in the reports provided by the organization are incorporated in the financial statements of user entities that submit pharmacy claims to the medical claims processor.	claims to the organization for processing.	
Report printing and mailing This organization prints the agency's electronic files containing financial reports for the agency and mails the reports to the agency. The information in the reports is incorporated into the agency's financial statements.	**Yes** The service provided by this organization is relevant to the agency's internal control over financial reporting because the information in the reports is incorporated in the agency's financial statements.	**Service Organization**
Report printing and mailing This organization prints the agency's electronic files containing financial reports for the agency and mails the reports to the agency. The information in the reports is incorporated into the agency's financial statements. The organization prints and mails the statements but the agency retains responsibility for the completeness and accuracy of the reports.	**No** Because the agency retains responsibility for controls over the completeness and accuracy of the reports, controls at this organization are not likely to be relevant to the agency's internal control over financial reporting.	**Vendor**
Document storage and record retention This organization picks up boxes of documents from the agency and stores them at its facility.	**No** Although this service is important to the agency's business and enables the agency to meet certain regulatory requirements, document storage and record retention services do not relate to the agency's internal control over financial reporting.	**Vendor**
Electric power This organization provides electric service to the agency	**No** Although important for the agency's continuing operations, the electric service does not relate to the agency's internal control over financial reporting.	**Vendor**
Customer Support Providing customers with post – sales support and service management.	**Yes** The service provided by this organization is relevant to the agency's internal control over financial reporting because the information is incorporated in the agency's financial statements.	**Service Organization**

Health care claims management and processing Provide medical providers, employers, third-party administrators, and insured parties of employers with systems that enable medical records and related health insurance claims to be processed accurately, securely, and confidentially.	**Yes** The service provided by this organization is relevant to the agency's internal control over financial reporting because the information in the reports is incorporated in the agency's financial statements.	**Service Organization**
Enterprise IT outsourcing services Manages networks/computing systems that reside within the third-party service provider location.	**Yes** The services provided by the third-party are relevant to the agency's internal control over financial reporting because controls over the network and computing systems where agency data resides are necessary for the agency's controls to operate effectively.	**Service Organization**
Financial Transaction Services Financial services with IT based transaction processing services (loan processing, peer-to-peer, payment processing, data analytics, asset management, etc.)	**Yes** The service provided by this organization is relevant to the agency's internal control over financial reporting because the information in the reports is incorporated in the agency's financial statements.	**Service Organization**

Source: AICPA SOC 1 Guide

Entities should also be aware of relationships that their service organization(s) has with other service organizations in support of their service delivery including but not limited to data centers, facilities management companies, printing companies, etc. The AICPA refers to these third-party organizations of service organizations as "subservice organizations" or "fourth parties. The agency is responsible for determining the responsibility of internal controls when a "fourth-party" organization is involved with the third-party relationship including consideration of user-agency controls. A subservice organization may be a separate entity that is external to the service organization or may be a related entity, for example, a subservice organization that is a subsidiary of the same company that owns the service organization. Management should evaluate the impact of the "fourth-party" organizations to determine if the operations are key to the internal controls of the agency.

Currently there are three types of Service Organization Control Examinations, which the entity and the service organization should evaluate to determine which one is applicable to the services being provided.

- SOC 1-Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting

- SOC 2- Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.
- SOC 3-Trust Services Report for Service Organizations (Based on SOC2 – but limited report)