NEW YORK STATE | Department of Health | Medicaid Redesign Team

System Security Plan Workbooks

Cloud Service Provider Guidance

August, 2016

Cloud Service Providers

According to the National Institute of Standards and Technology (NIST), a *Cloud Service Provider* is one that:

> “enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management.”

The DOH definition of *Cloud Service Provider* expands upon the NIST definition and includes vendors that may not completely meet the NIST definition but provide computing resources in a *multi-tenant environment*. A multi-tenant environment is one in which a third-party provides similar computing resources to several of its customers, and at least a portion of those resources are shared by multiple customers.

- For example, if the third-party provides a dedicated virtual server to the PPS, but that server utilizes a volume on a shared Storage Area Network, then the third-party provides multi-tenant services and would be considered a Cloud Service Provider, for the purposes of the PPS completing the DOH SSP.

SSP Controls for Cloud Service Providers

- SSP controls are either completely dedicated to Cloud Service Providers or have individual items and guidance that apply to Cloud Service Providers. These controls and items are preceded by “(For CSP Only)”.
- Even if an organization does not make use of a Cloud Service Provider, controls and individual items marked as such should be reviewed by the PPS to ensure that those items don’t have meaning to their specific implementation.

Note:

Controls containing items that apply to Cloud Service Providers often have items that are not marked “(For CSP Only)” and would apply to all organizations, including those that are not making use of a Cloud Service Provider.

Providing Control Information for Cloud-Based Systems

- When a third-party provides computing resources to a PPS, the controls that apply to those outsourced resources need to be explained and have evidence provided in the workbooks.
- Many Cloud Service Providers consider information related to their controls as intellectual property and may not be willing to permit DOH to review information and artifacts related to controls without a non-disclosure or similar agreement with DOH.
- The PPS is responsible for coordinating the request for the necessary agreements with the Cloud Service Provider and DOH, to enable controls to be reviewed.
- In lieu of having the Cloud Service Provider supply artifacts, the PPS may create documentation and retrieve artifacts from the outsourced system, to respond to the SSP controls, as practicable.

FedRAMP System Security Plans

- Cloud Service Providers that provide FedRAMP-compliant computing resources have developed a FedRAMP System Security Plan that can be used to provide explanations and artifacts for the DOH SSP.
- The FedRAMP SSP is similar to the DOH in general format and controls, but the DOH SSP includes additional language, specific to NYS policies and standards.
- The FedRAMP SSP is often considered intellectual property by Cloud Service Providers, since it contains some of the most sensitive security information for the Cloud Service Provider’s infrastructure and services.
- Not all Cloud Service Providers offer FedRAMP-compliant services. Such organizations may not provide System Security Plans that describe the controls for their infrastructure and applications. The PPS is responsible for working with these organizations to complete the DOH SSP for applicable controls.
- DOH strongly recommends the use of Cloud Service Providers that offer FedRAMP-compliant services and to make use these services.

Understanding the PPS Role in Completing the SSP

- In the Cloud Service Provider’s FedRAMP SSP, the Cloud Service Provider defines the controls and sections of controls that are the responsibility of the “customer”. In these sections the PPS needs to provide its own explanations and artifacts that describe how the PPS is implementing these items.

- For the control sections where the Cloud Service Provider has assumed ownership, the Cloud Service Provider’s FedRAMP SSP may be referenced by the PPS in its DOH SSP for those sections, but the PPS must ensure that the Cloud Service Provider’s SSP provides the necessary explanations and artifacts for the associated items.

- A matrix of responsibilities for SSP controls and control sections that are assigned to the Cloud Service Provider and those assigned to the PPS must be provided, so that the delineation of responsibilities can be understood, during the DOH review. Each control in each workbook and each bulleted requirement must be addressed, as applicable. Cloud Service Providers offering FedRAMP-compliant services often provide this matrix as a publicly available download, and this document should be included with the SSP submission to DOH.

- DOH is only capable of reviewing controls where it has access to associated explanations and artifacts. The PPS should ensure that all necessary information is included in the DOH SSP submission, for controls and items for which the Cloud Service Provider is responsible.

Control example for organizations using a Cloud Service Provider (CSP)

RA-3 – Risk Assessment (Moderate)

Control

The organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the

b. Destruction of the information system and the information it processes, stores, or transmits;

c. Documents risk assessment results in the applicable security plan;

d. (For CSP Only) This line would only apply if using a Cloud Service Provider

Implementation Standard(s)

1. (For CSP only) For service providers, the organization documents risk assessment results in the security assessment report.
2. (For CSP only) For service providers, the organization reviews risk assessment results at least every three (3) years or when a significant change occurs

Guidance

Clearly defined authorization boundaries are a prerequisite for effective risk assessme and impact to organizational operations and assets, individuals, other organizations, a assessments also take into account risk from external parties (e.g., service providers, individuals accessing organizational information systems, outsourcing entities).

(For CSP only) Significant change is defined in NIST Special Publication 800-37 Revis

Reference(s): HIPAA, NYS Policies and Standards, NIST SP 800-53 […]

All lines must be addressed in the control explanation. It may be necessary to have the CSP participate in completing the control explanations and providing relevant artifacts.

All implementation standards need to be addressed.

NOTES:

It may be necessary to request information from the Cloud Service Provider to complete the control descriptions and provide the required artifacts to demonstrate that the control is in place.

CSPs may require NDAs or contractual protections before releasing this information in a form that can be obtained by DOH for the SSP review.

It is the responsibility of the PPS to work with the CSP to make this information available to DOH for review or to provide equivalent information on the CSP's control environment to demonstrate in-place controls.

This control has been modified for illustrative purposes.
See SSP RA workbook for actual requirements

Example: Control implementation section

Fully explain control implementation *(or fully explain why control requirement is not applicable)*

Status: IMPLEMENTED

Applicability:

a. Primary Application and Secondary Application “PHIReporter”

b. This control does not apply to Secondary Application “Widget,” because of reason: *well-explained and credible business reason.*

Description:

Cloud Service Provider responsibilities: (a) (b) (c) and (d) for the part of the system that is hosted by the CSP. Implementation details and artifacts provided in Cloud Service Provider SSP (Provided with the SSP submission), control RA-3.

PPS responsibilities: (a) (b) (c) and (d) for the parts of the system hosted by the PPS, and for performing risk assessments for the overall system and its use for the PPS business. Specifics include:

Risk assessment process for the PPS organization utilizes a risk assessment process that adheres to NIST 800-30 and is attached. Risk assessments are conducted for PHI Reporter annually and following meaningful changes to the system, as per the attached policy. The record of previous risk assessments for PHI Reporter are attached. A sample risk assessment is attached, along with a plan for remediating issues with dates and associated outcomes.

Risk assessment results are reported to leadership, when completed. An example report is attached.

The risk assessment process is reviewed and updated annually and following significant changes to the threat landscape. The record of such changes is included in the risk assessment procedure, attached.

Example: Control implementation section

Attachments:

- Cloud Service Provider SSP with attached artifacts
- Risk assessment procedure
- Risk assessment policy
- Example completed risk assessment
- Example remediation plan with dates and outcomes
- Example risk assessment report
- Record of risk assessments conducted for PHI Reporter, with dates

Responsible for Control Implementation: *(document the organizational component or contractor responsible for supporting and maintaining the control.)*

The controls are supported internally by the organization. The Organization’s Compliance department is responsible for supporting and maintaining the applicable controls.