Requirements to Use Cloud Services [1]

Topics:
cloud [2], procurement [3], SaaS [4], EOE [5]

SA-14-003 Requirements to Use Cloud Services

Issue Date: 11/01/2013

Revision Effective Date: 11/01/2013

PURPOSE

The National Institute of Standards and Technology (NIST) defines ?cloud computing? as a computing model for ?enabling 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 effort or service provider interaction.? Cloud computing service models include network access to software applications (Software as a Service, SaaS), network access to an environment for customers to use, build and operate their own software (Platform as a Service, PaaS) or network access to traditional computing resources such as processing power and storage (Infrastructure as a Service, IaaS). The State of Georgia enterprise operational environment (EOE) provides infrastructure and network services in a proprietary private cloud environment which satisfied the requirements of PaaS and IaaS. State enterprise standard SO-10-003 ?Enterprise Operational Environment? establishes the EOE as the standard operational environment for state agencies and provides a methodology for an agency to pursue a justified exemption from the standard.

This standard provides governance and expectations concerning State governmental agencies use of cloud services.

STANDARD

- Cloud services (SaaS, PaaS or IaaS) are not allowed for agency use except as an exemption from SO-10-003 or according to the provisions of this standard. Agencies are allowed to Request an Exemption for a specific cloud service by both SO-10-003 and this standard.
- A Request for Exemption from SO-10-003 for any Cloud service shall be submitted on a form approved by GTA and include the following documentation:
    - Description of the project for which an exemption is requested. The description shall include the name of the service (application), its function, and its intended use by the agency. In addition, the description shall identify the hosting entity, the entity that provides the service (developer) and supports the service (maintains, provides trouble support, etc.), and the location at which the service will be hosted.
    - Assurance that the agency has submitted an APR and Business Case to GTA, or information in lieu of these items required by the Request for Exemption form.
    - A statement from the Senior Agency Information Security Officer that includes:

        - A security impact categorization of the service,
        - Assurance that the agency?s security needs are met by the proposed vendor,
        - Any unresolved gaps between agency?s security needs and security provisions of the proposed vendor are acceptable to the agency.
    - The cloud service provides appropriate back-up and recovery services to meet the needs of the agency and that state data can be retrieved should it be necessary.
- A cloud application to be used to provide for agency business (software that provides for an agency business service, not application development or testing) is allowed for agency use, without the agency first securing an exemption from enterprise standard SO-10-003 ?Enterprise Operational Environment?, provided that the application also meets the following criteria:
    - Data to be deployed to the cloud service application has a security categorization of LOW.
    - The cloud application is self-contained, or it shares data, services and business processes with other systems in the State environment (enterprise integration) via State operated integration middleware.
    - The agency obtains, at least annually, from the cloud application provider, attestment to its security provisions with a SSAE16 Report of assessment prepared using industry accepted methodology against controls specified for LOW impact systems in NIST 800-53.
    - The agency information security officer has compared the security provisions of the third party to the needs of the business process and has provided a written opinion that the security, privacy and confidentiality risks remaining are acceptable.
    - The cloud application provides for appropriate back-up and recovery services and all state data is retrievable when required.
    - The agency has defined an appropriate records retention schedule for the records used and/or generated with the cloud service as provided for by State Law; Federal Laws and Regulations; and enterprise IT and security policies and standards.
- A completed copy of the form ?Deployment of Cloud Service? for all cloud services enabled for agency use shall be forwarded to GTA?s Enterprise Governance and Planning Division within thirty (30) days prior to the deployment of the service.

TERMS and DEFINITIONS

SSAE16 ? Statement on Standards for Attestation Engagements No. 16 (SSAE16) replaces Statement on Auditing Standards No. 70 (SAS 70). It is a professional standard issued by American Institute of Certified Public

Accountants as guidance to practitioners engaged to examine and report on a service organization?s controls over the services it provides to user entities when those controls are likely to be relevant to user entities? internal controls over financial reporting.

SaaS (Software as a Service) - Cloud computing service models include network access to business software applications hosted in the cloud by a third party. This model allows costs of software development and hosting to be shared among subscribers. Business software in this category is often configurable to a limited extent with standard options offered to all subscribers.

PaaS (Platform as a Service) - Cloud services which permit network access to an environment for agencies to use, build or operate their own software.

IaaS (Infrastructure as a Service) - Cloud services which permit network access to traditional computing

resources such as processing power and storage.

Source URL: https://gta.georgia.gov/psg/article/requirements-use-cloud-services