

Everything as a Service: the New Normal in Procurement

Steve Nichols
Georgia Technology Authority
May 9, 2016

Thesis

- More and more procurements will involve software as a service
- Some will be obvious
- Some will not be obvious

Trends in Georgia Procurements

- Small apps going to cloud
- Large apps, apps with regulated data staying in state data center
- Cloud is primarily software as a service (SaaS)
- Driven by business
- Procurements that don't look like technology, but have a SaaS component

Practical Advice

Rest of my talk is split into two buckets:

- RFPs – requirements for services
- Contracts – terms & conditions for services

Cloud Ts & Cs Best Practice Guide

- Service Models
- Data
- Breach Notification
- Security
- Audits
- Operations



<http://www.govtech.com/cdg/>

RFP - On Premise, or Cloud Hosted?

- First thing: do you even have a choice?
- Three likely outcomes:
 - Premise only
 - Cloud only
 - Either/or

GTA and cloud

- SO-10-003 Enterprise Operational Environment
 - You are required to host with GTA; you can get an exemption; lists 10 requirements for exemption
 - <http://gta.georgia.gov/psg/article/enterprise-operational-environment>
- SA-14-003 Requirements to Use Cloud Services
 - Details when you need an exemption from SO-10-003 and how to apply
 - <http://gta.georgia.gov/psg/article/requirements-use-cloud-services>

RFP – Expect Layers of Vendors

- Common to see SaaS vendors using IaaS vendors or co-location vendors to provide the data center
- Be sure to include language in the RFP about disclosing who the subcontractors are
- Think about flow-down requirements

RFP - SSAE 16: a Crash Course

- SOC 1
 - Type 1
 - Type 2 – *you might end up with this, too*
- SOC 2
 - Type 1
 - Type 2 – *this is the one you'll be interested in*
- SOC 3

What about FedRAMP?

- FedRAMP = Federal Risk and Authorization Management Program
- Three ways to get FedRAMP certified:
 - JAB Provisional Authorization
 - Agency Authorization
 - CSP Supplied Package
- There are 44 companies certified as compliant (as of March, 2016)

RFP - Location of your Data

- GTA's position on offshore data
 - SS-15-002.01 Data Storage Location
 - <http://gta.georgia.gov/psg/article/data-storage-location>
 - *All State data must be processed, stored, transmitted and disposed of onshore (within the jurisdiction of the United States).*
- You'll want to cover a couple of additional edge cases here in the RFP
 - Data stored on portable devices
 - Location of personnel or contractors who are accessing your data remotely to provide technical support

RFP – External Interfaces

- Easy to miss in an RFP
- Suppliers need to know:
 - What interfaces?
 - Real time or batch?
 - Formats?
 - Regulatory requirements? (e.g. encryption)

RFP – Disaster Recovery

- DR in SaaS systems use different strategies
- You are largely at the mercy of your provider
- Third party cloud backup providers

RFP - Information Security

- State of Georgia position
 - PS-08-005 Enterprise Information Security Charter
 - The State follows the Federal Information Security Management Act (FISMA) and supporting documentation from NIST
 - <http://gta.georgia.gov/psg/article/enterprise-information-security-charter>
- At a minimum, put this into your RFP
- There are a lot of other frameworks out there...
 - Suppliers that do a lot of federal business
 - Suppliers that don't

Contracts

- Contracts will be mostly silent on the things I'm going to tell you about
- Compliance information and operational processes will likely be on website
- Security details will be in SSAE 16 SOC report
- Put your reading glasses on

Contract - Data Ownership

- The public jurisdiction owns all of its data.
- The service provider will not access the data except as needed to do the work of the contract.
- The public jurisdiction owns all data obtained by the service provider in the performance of this contract.
- Data location – repeat the U.S. only language in the contract

Contract - Security

- The service provider will perform background checks on staff, including subcontractors.
- The service provider shall perform an independent audit of its data centers at least annually.
- That the service provider will make a version of that audit available to you (hopefully as a SSAE 16 SOC 2 report)
- Subcontractors!

Contract - Plan for your exit

- Orderly retreat or rout?
- Nirvanix as a cautionary tale...
 - Cloud storage provider (public, private, and hybrid), founded in 2007
 - Notified customers to get their data on Sept. 16th, 2013
 - Deactivated website on Sept. 28th, filed for Chapter 11 bankruptcy on October 1st.

Contract - Import/Export of Data

- The public jurisdiction can import or export its data whenever needed.
- Termination for convenience: be prepared for 30 days

Contract - Termination/Suspension

- The service provider will not erase the public jurisdiction's data in the event of a suspension or when the contract is terminated.
- Specific time periods are established where data will be preserved by the service provider.
- The service provider will destroy data using a NIST-approved method when requested by the public jurisdiction.

Cloud Ts & Cs Best Practice Guide



<http://www.govtech.com/cdg/>

Questions?

Steve Nichols

For a copy of this deck or any additional questions: cto@gta.ga.gov