I. “Head in the Clouds” Syndrome

Introduction to cloud hosting and Software-as-a-Service
The “Who”

- **Division of State Audit**
  - Legislative branch; Independent IS/IT State Agency Audits

- **TN Executive Branch**
  - Centralized IT Service Bureau – Strategic Technology Solutions

- **Information Systems Council**
  - Legislative oversight body for TN IT projects
State Agency Audits

- State Agency Financial & Compliance
- Performance (sunset)
- State Higher Education
- Single Audit (Federal)
"Someone else's computer!"

(NIST) On-demand network access to a shared pool of configurable computing resources with minimal management effort.
Don’t SaaS me!

**SaaS**

- Software & end-user applications:
  - Applications
  - Data

**PaaS**

- Hardware and software tools; often for developers:
  - IaaS plus middleware & Operating systems
  - Scalable

**IaaS**

- IT Building blocks:
  - Storage
  - Networking
  - Virtualization

- Touchnet
- Accufund
- Jaggaer
- RackSpace
- Amazon Web Services
- Microsoft Azure
Deployment Models

- On-Premises
- Hybrid
- Cloud

Agency still owns & has responsibility for security of their data!
Trends in Tennessee’s IT Landscape

- More outsourcing of IT functions
- Cost / benefit
- Updates to IT cloud hosting contract language
## SaaS Growth Projections

### Table 1. Worldwide Public Cloud Service Revenue Forecast (Billions of U.S. Dollars)

<table>
<thead>
<tr>
<th>Service</th>
<th>2017</th>
<th>2018</th>
<th>2019</th>
<th>2020</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Business Process Services (BPaaS)</td>
<td>42.2</td>
<td>46.6</td>
<td>50.3</td>
<td>54.1</td>
<td>58.1</td>
</tr>
<tr>
<td>Cloud Application Infrastructure Services (PaaS)</td>
<td>11.9</td>
<td>15.2</td>
<td>18.8</td>
<td>23.0</td>
<td>27.7</td>
</tr>
<tr>
<td>Cloud Application Services (SaaS)</td>
<td>58.8</td>
<td>72.2</td>
<td>85.1</td>
<td>98.9</td>
<td>113.1</td>
</tr>
<tr>
<td>Cloud Management and Security Services</td>
<td>8.7</td>
<td>10.7</td>
<td>12.5</td>
<td>14.4</td>
<td>16.3</td>
</tr>
<tr>
<td>Cloud System Infrastructure Services (IaaS)</td>
<td>23.6</td>
<td>31.0</td>
<td>39.5</td>
<td>49.9</td>
<td>63.0</td>
</tr>
<tr>
<td>Total Market</td>
<td>145.3</td>
<td>175.8</td>
<td>206.2</td>
<td>240.3</td>
<td>278.3</td>
</tr>
</tbody>
</table>

Dated Sept. 2018
**Enterprise SaaS Vendor Market Share & Revenue Growth**

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Market Share</th>
<th>Annual Growth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
<td>15%</td>
<td>45%</td>
</tr>
<tr>
<td>Salesforce</td>
<td>10%</td>
<td>25%</td>
</tr>
<tr>
<td>Adobe</td>
<td>8%</td>
<td>32%</td>
</tr>
<tr>
<td>Oracle</td>
<td>7%</td>
<td>43%</td>
</tr>
<tr>
<td>SAP</td>
<td>6%</td>
<td>36%</td>
</tr>
<tr>
<td>Next 10</td>
<td>10%</td>
<td>28%</td>
</tr>
</tbody>
</table>

*Worldwide Market Share - Q2 2018*

*Source: Synergy Research Group*
Number of Apps per Company

Other SaaS Trends

- Decentralization of ownership for SaaS
  - Visibility is critical to proper management!

- High SaaS App turnover
  - Improves flexibility to adapt

II. Roles & Responsibilities

Role of Audit vs. Management’s Responsibilities
The “Danger Zone” Doesn’t Change

Outsourcing does NOT eliminate risks affecting your data!
Takin’ Care of Business

- Agency management is accountable for their **data** & the completion of their **mission** to serve public interest

- Outsourcing shifts **HOW** management should manage risk & ensure safeguards are in place

  *Doesn’t mean they will agree with your audit approach!*
“If you’re buying a car...”
Managements’ Responsibilities

- Governance, Risk, and Compliance (GRC) crucial in new landscape

- Risk Assessment/GRC process should include consideration of outsourced IT services & recognition of data sensitivity

- Security requirements should be dependent upon data classification & sensitivity of agency’s mission to disruption
Auditor’s Role

- Audit’s job is to ensure Management has GRC process in place; not to perform GRC for the agency!

- Audit should ensure management has evaluated risks & put safeguards in place where appropriate
“Authority AlwaysWins!”

- **GAO Green Book** *(Standards for Internal Control in the Federal Government)*
- **NIST 800-53 (Rev. 4)*
- **GAO FISCOM** *(Federal Information System Controls Audit Manual)*
- **ISACA Publications & COBIT*
Contracts

- Management should ensure appropriate contract requirements:
  - Sufficient data security & physical location
  - Audit clause
  - Security certification / authorization; SOC Audit requirement

- Analysis of data type/sensitivity & criticality of business function should drive contract requirements
Managements’ Responsibilities for SaaS

- Do they obtain and review SOC audit reports?
- Does management understand *complementary user entity controls* & have they placed controls in operation?
- Has management demonstrated data integrity through any type of reconciliation process?
Securing SaaS

- Managing user access to the application & data
  - Password controls / authentication methods

- Configuring ‘transaction’ workflows to align with policies

- Reconciling transactions in SaaS app vs. other systems

- Coordinating with SaaS vendor to test/validate app changes
“Who are you?” (I really wanna know!)

- Consider the SaaS application “owners” and Admins

  - Potential risk if non-technical personnel are responsible for configuring SaaS security

  - Potential risk if IT department is not engaged with data custodians that manage SaaS app
III. Tools for Auditors

Contractual Obligations, Security Certifications, & Audit Reports
Contractual Requirements

- Ownership & location of data?
- Key SLA’s?
- Right to audit clause?
- Security Requirements for Software &/or Data Center hosting vendor(s)?
Security Certifications

- **PCI**
  - Compliance Reporting over Data Security Standards (DS) Framework

- **ISO**

- **FedRAMP**
  - “Authorization” (low, medium, or high) level based on independent third-party’s Security Assessment Report
SOC Audit Reports

- Issued by independent CPA firm
- SOC Reporting Options: SOC1, SOC2, SOC3
- SOC Types: Type 1 or Type 2
## SOC “Reporting Options”

<table>
<thead>
<tr>
<th>SOC 1</th>
<th>SOC 2</th>
<th>SOC 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSAE No. 18 (supercedes No. 16)</td>
<td>AT 101 &amp; TSP 100</td>
<td>AT 101 &amp; TSP 100</td>
</tr>
<tr>
<td>Internal Control Over Financial Reporting</td>
<td>Operational Controls Trust Services Principles</td>
<td>Operation Controls Trust Services Principles</td>
</tr>
<tr>
<td>Restricted Use – Customers &amp; their Auditors</td>
<td>Restricted Use – Customers, their auditors, specified parties</td>
<td>General Use – Publicly Available</td>
</tr>
</tbody>
</table>
### SOC Report “Types”

<table>
<thead>
<tr>
<th><strong>Type 1</strong></th>
<th><strong>Type 2</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Design</strong> of controls only; no assurance over operating effectiveness</td>
<td><strong>Design &amp; operating effectiveness</strong> of controls</td>
</tr>
<tr>
<td>For a <strong>Point-in-Time</strong></td>
<td>Covers a <strong>Period of Time</strong></td>
</tr>
<tr>
<td>Does NOT include details of test work</td>
<td>Includes <strong>detailed test work</strong> results</td>
</tr>
</tbody>
</table>
SOC Gap / Bridge Letters

What if SOC audit report does not cover audit period?

- Does not provide assurance

- Managements’ written statement about control environment

- Should be considered if SOC audit does not cover entire period
Other Factor to Consider

- SaaS Vendor’s financial position & market recognition

- Availability of business continuity plans (BCPs), disaster recovery plans (DRPs) and robust backup procedures

- Availability of other policies / plans for security management
Inherent SaaS Risk Factors

- Data ownership, portability, & disposal
- Ease to contract for SaaS
- Lack of visibility into SDLC & security considerations
- Lack of control over software patch release process
- Identity/access management
- Web browser vulnerabilities
IV. How to Use Available Tools

Audit Scope/Objectives, Contractual obligations, SOC Audit Reports
Hammer Time!

- What is your audit objective & scope?
- Do you need evidence of the operating effectiveness of controls?
- What has management already documented?
  - Risk Assessments
  - Security Assessments or Plans
  - Security Compliance Reports/Certifications?
Direct Interaction with Vendor

- If contract permits & vendor/agency agree, consider working directly with the cloud vendor.

- Consider limitations of audit clause in contract

- Requires good relationship between vendor & agency management
If available, obtain and review SOC Audit Reports

- Does the SOC report’s scope address your needs?

Take special note of:

- Service Auditor’s Opinion & Test Work Conclusions (Type 2 only)
- Tests of Controls in Type 2 report
- User Entity Controls

Consider implications of poor internal controls at SaaS vendor!
Other Security Certifications / Assessments

- Consider applicability to your audit objectives
  - *Do you need evidence of operating effectiveness?*

- Consider whether these certifications / assessments provide any actual audit *assurance* about design or operating effectiveness of controls
Concluding – *Easier Said than Done*

Do these reports / certifications / security assessments provide you with *sufficient evidence* (or *assurance*) to achieve your objectives?
SOC Report Evaluation Template

- Standardized form to document:
  - SOC Report general information (service auditor, scope, etc.)
  - SOC Report opinion
  - Period covered by the report
  - Service auditor’s professional reputation
  - Use of subservice organizations
  - Identify control objectives &/or results of tests of operating effectiveness
  - Complementary User Entity controls
  - Conclusion
V. Tales from the Trenches

Case Studies from Recent Tennessee Agency Audits
Scenario 1 – No SOC Audit Report

TN Department of Education (TDOE) and Department of Human Services (DHS) used a SaaS vendor’s information system services to support federal programs.

Same SaaS Vendor for two SaaS Applications:
- (TDOE) TN Meals, Accounting, and Claiming (TMAC)
- (DHS) TN Information Payment System (TIPS)
Scenario 1 – No SOC Audit Report

- Contract did not require SOC audit report;
  - Established before changes in contract language

- SaaS Vendor did not have other security certification(s)

- Agency did not evaluate SaaS vendor’s controls

- IaaS subservice organization SOC Audit report was available
Scenario 1 – No SOC Audit Report

Our Response:

- Reported internal control finding for lack of:
  - Management’s own evaluation/assessment of SaaS vendor’s controls for purpose of risk management/assessment
  - Recommended internal review of SaaS vendor controls if SOC audits and/or security certifications were not available
  - “Unable to achieve our audit objectives related to critical system controls”
Scenario 2 – SOC Audit Report Qualified

- SaaS Vendor for large agency was subject to SOC audit and provided report upon our request

- Agency management had NOT obtained & reviewed the SOC audit report prior to our audit

- SOC Audit Report opinion was qualified; reported several internal control deficiencies
Scenario 2 – Qualified SOC Audit Report

Our Response:

- Reported internal control finding:
  - Management did not obtain & review available SOC audit report; were unaware that SaaS vendor’s SOC audit report contained qualified opinion
  - Management did not perform their own evaluation/assessment of SaaS vendor’s controls for purpose of risk assessment & mitigation
Scenario 3 – SaaS vs IaaS SOC Audits

- Several large agencies use SaaS vendors that outsource “data center colocation services” to a subcontractor.

- Some contracts have required SOC audit report for IaaS vendor but not for SaaS vendor.

- We have reported control weaknesses if management does not assess risk of SaaS vendor’s internal control environment separately from IaaS vendor.
Scenario 3 – SaaS vs IaaS SOC Audits

Our Response:

- Reported Internal Control Finding
  - Recommended revision of contract requirements upon renewal
  - Agencies to perform their own review/assessment of SaaS vendor controls
Scenario 4 – “We don’t Need no Education”

- TN DOE implemented new system, Nextera, for online testing at public schools in 2017 & 2018.

- Questar Assessment Inc. designed, implemented online testing platform, Nextera, and executed paper-based testing.
Scenario 4 – “We don’t Need no Education”

- Questar’s services were significantly disrupted during Spring 2018 testing window
  - Suspicion of cyberattack!

- Generated media buzz and public outcry; damage to trust of public and legislators

*Technical issues compounded by fiber line cut during test window*
Scenario 4 – “We don’t Need no Education”

- After months of investigating by TN State Audit, agency, and 3rd party cybersecurity firm
  - No evidence of cyberattack
  - SaaS vendor made ‘unauthorized’ text-to-speech technology change
  - Infrastructure software misconfigurations led to most performance problems

- State financially penalized SaaS vendor for performance issues; SaaS vendor’s contract in jeopardy

- Reported multiple internal control findings in 2018 Audit Report
Scenario 5 – Vendor Unwilling to have SOC Audit

- SaaS vendor for DHS & DOE was unwilling to pay for SOC audit; contract did not require SOC audit.

- After several years of repeat findings, management of agency collaborated with SaaS vendor and vendor has agreed to pay for SOC audit.
Lessons Learned

✓ Management is responsible for
  - their data & completing their mission
  - identifying risks to their data & business processes – even if performed by SaaS
  - implementing controls to address identified risks

✓ Healthy relationship between SaaS vendor and agency is crucial in a crisis

✓ “Good” contracts & SLAs are essential to effective relationship with SaaS vendors
Looking to the Future

- TN Comptroller's Office is coordinating with State Agencies to improve contract language requirements for cloud/SaaS vendors
  - SOC Audit Reports
  - ISO
  - FedRAMP Authorization
Questions?
Contact Information

Jeff White, CPA, CISA
Legislative IS Auditor

Office of the Comptroller of the Treasury
Division of State Audit
Cordell Hull Building
425 Fifth Avenue North
Nashville, TN 37243

Phone: 615-747-5300
Email: Jeff.White@cot.tn.gov