AUDIT REPORT

Cloud Software as a Service (SaaS) Procurement and Governance Audit

June 9, 2016
Table of Contents:

**Executive Summary**

Background  
Audit Objectives and Scope  
Management’s Assessment and Reporting on Controls  
Audit Opinion

**Appendix**

Definitions  
Issue Classifications  
Distribution  
Audit Performed By
Executive Summary

Background

Cloud Software as a Service (SaaS) is a software model in which a third-party provider hosts applications and makes them available to customers through an Internet connection. As opposed to traditional on-premises software which requires organizations to purchase, install and maintain IT hardware and software, SaaS providers host software at their locations. Strategically, the use of SaaS by an organization allows IT resources to be deployed in accordance with its business objectives.

Citizens utilizes both SaaS and traditional on-premises applications. The Citizens’ IT Strategic Plan addresses the consideration of SaaS as follows: “In selection of systems, or as we have lifecycle opportunity with current systems, we will evaluate options for external hosting (assess cloud options). Systems as a Service (SaaS), or other external hosting options will be assessed and are preferred where there is a good fit with overall cloud strategies, when risks can be well-managed, where integration objectives are supported, and when cost/benefit analysis is favorable.”

IT has also developed a cloud strategy which includes a phased approach for SaaS implementation including procurement and governance. In carrying out the SaaS strategy, Citizens is not actively seeking SaaS providers to replace existing solutions. However, as opportunities arise, SaaS providers will be considered as appropriate.

In 2015, the Citizens’ Vendor Management Office (VMO) developed a SaaS Decision Framework to put structure around the procurement and governance of SaaS applications. The framework, approved by the Executive Leadership Team in June 2015, identifies organizational departments involved in the procurement and governance process, as well as key points where the viability of potential SaaS solutions is determined. In addition to SaaS based applications, IT is also evaluating SaaS based options for disaster recovery and potentially the ERP solution. VMO Management indicated there were roughly thirteen SaaS vendors at the time of the audit.

Audit Objectives and Scope

The objective of this audit was to evaluate the adequacy and effectiveness of controls related to the procurement and governance of SaaS implementations. The scope of the audit included an assessment of:

- Alignment of the SaaS Decision Framework to cloud industry guidance
- Review of the IT Strategic Plan for inclusion of a SaaS adoption strategy
- Controls around the SaaS procurement process and application of the SaaS Decision Framework
- Procurement of SaaS vendors, including cross-functional evaluation of SaaS viability for concept proposals and scoring of SaaS vendor solicitations
- Governance of SaaS vendors, including contract manager monitoring of SaaS vendor agreements for Service Level Agreement (SLA) performance, vendor billings, and receipt and review of SOC reports. Additionally, the SaaS vendor data breach notification process was evaluated
- Administration of Citizens’ access to SaaS vendor systems

The scope of this audit did not include the vendor payment process nor re-performance of contract manager SaaS billing validation.
Executive Summary

Management’s Assessment and Reporting on Controls

OIA met with Management to determine if there were any internal control issues related to the audit scope that Management would like to report. VMO stated a retroactive review of SaaS contracts for information security and data privacy language was being performed at audit inception, to ensure SaaS specific terms and conditions were included. The project was completed during the course of the audit.

Audit Opinion

Based upon our audit work, the overall effectiveness of the SaaS Decision Framework and related controls evaluated during the audit of Cloud SaaS Procurement and Governance is rated as Needs Minor Improvement.

With the development and implementation of a SaaS strategy and decision framework, the VMO was able to implement a major step in strengthening Cloud SaaS procurement and governance controls. Our work, however, indicated specific areas where opportunities for improvement were noted including:

- **Procedures to complement the SaaS Decision Framework have not been formally documented to ensure consistent use.** Detailed procedures have not been created to support the SaaS Decision Framework for process areas that are specific to the review of cloud providers being considered in a solicitation or purchase. Contents that are missing, based upon industry guidance, include the formal assignment of roles, responsibilities and deliverables for each process step, vendor risk assessment requirements and the potential inclusion of additional vendor requirements in the service level agreement as output from the risk assessment. As well, an assurance process should be developed and implemented to validate ongoing compliance with the SaaS Decision Framework.

- **A formalized process is not in place to ensure consistent use of the VMO SaaS Decision Framework when SaaS is purchased through a purchase order.** There is not a documented procedure to ensure that procurements follow the SaaS Decision Framework for non-enterprise concept proposal cloud services less than $35K, or more than $35K, if obtained via a state term contract. VMO and the Purchasing department coordinate to obtain approvals for software purchases requested through the IT service desk application. However, if a software purchase is for cloud services, a formalized process is not in place to ensure that the SaaS Decision Framework would be applied.

We would like to thank management and staff for their cooperation and professional courtesy throughout the course of this audit.
Appendix 1

Definitions

Audit Ratings

Satisfactory:
The control environment is considered appropriate and maintaining risks within acceptable parameters. There may be no or very few minor issues, but their number and severity relative to the size and scope of the operation, entity, or process audited indicate minimal concern.

Needs Minor Improvement:
The number and severity of issues relative to the size and scope of the operation, entity, or process being audited indicate some minor areas of weakness in the control environment that need to be addressed. Once the identified weaknesses are addressed, the control environment will be considered satisfactory.

Needs Improvement:
The audit raises questions regarding the appropriateness of the control environment and its ability to maintain risks within acceptable parameters. The control environment will require meaningful enhancement before it can be considered as fully satisfactory. The number and severity of issues relative to the size and scope of the operation, entity, or process being audited indicate some noteworthy areas of weakness.

Unsatisfactory:
The control environment is not considered appropriate, or the management of risks reviewed falls outside acceptable parameters, or both. The number and severity of issues relative to the size and scope of the operation, entity, or process being audited indicate pervasive, systemic, or individually serious weaknesses.
### Issue Classifications

<table>
<thead>
<tr>
<th>Control Category</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Financial Controls</strong> (Reliability of financial reporting)</td>
<td>• Actual or potential financial statement misstatements &gt; $10 million&lt;br&gt;• Control issue that could have a pervasive impact on control effectiveness in business or financial processes at the business unit level&lt;br&gt;• A control issue relating to any fraud committed by any member of senior management or any manager who plays a significant role in the financial reporting process</td>
<td>• Actual or potential financial statement misstatements &gt; $5 million&lt;br&gt;• Control issue that could have an important impact on control effectiveness in business or financial processes at the business unit level</td>
<td>• Actual or potential financial statement misstatements &lt; $5 million&lt;br&gt;• Control issue that does not impact on control effectiveness in business or financial processes at the business unit level</td>
</tr>
<tr>
<td><strong>Operational Controls</strong> (Effectiveness and efficiency of operations)</td>
<td>• Actual or potential for public censure, fines or enforcement action (including requirement to take corrective actions) by any regulatory body which could have a significant financial and/or reputational impact on the Group&lt;br&gt;• Any risk of loss of license or regulatory approval to do business&lt;br&gt;• Areas of non-compliance identified which could ultimately lead to the above outcomes&lt;br&gt;• A control issue relating to any fraud committed by any member of senior management which could have an important compliance or regulatory impact</td>
<td>• Actual or potential for public censure, fines or enforcement action (including requirement to take corrective action) by any regulatory body&lt;br&gt;• Areas of non-compliance identified which could ultimately lead to the above outcomes</td>
<td>• Actual or potential for non-public action (including routine fines) by any regulatory body&lt;br&gt;• Areas of non-compliance identified which could ultimately lead to the above outcome</td>
</tr>
<tr>
<td><strong>Compliance Controls</strong> (Compliance with applicable laws and regulations)</td>
<td>Such an issue would be expected to receive immediate attention from senior management, but must not exceed 60 days to remedy.</td>
<td>Such an issue would be expected to receive corrective action from senior management within 1 month, but must be completed within 90 days of final Audit Report date.</td>
<td>Such an issue does not warrant immediate attention but there should be an agreed program for resolution. This would be expected to complete within 3 months, but in every case must not exceed 120 days.</td>
</tr>
<tr>
<td>Remediation timeline</td>
<td>Such an issue would be expected to receive immediate attention from senior management, but must not exceed 60 days to remedy.</td>
<td>Such an issue would be expected to receive corrective action from senior management within 1 month, but must be completed within 90 days of final Audit Report date.</td>
<td>Such an issue does not warrant immediate attention but there should be an agreed program for resolution. This would be expected to complete within 3 months, but in every case must not exceed 120 days.</td>
</tr>
</tbody>
</table>
Appendix 3

Distribution

Addressee(s)  Stephen Guth, VP – Vendor Management

Copies  

**Business Leaders:**
Barry Gilway, President/CEO/Executive Director
Kelly Booten, Chief – Systems and Operations
Curt Overpeck, Chief Information Officer
John Rollins, Chief Risk Officer
Dan Sumner, Chief Legal Officer & General Counsel
Christine Turner Ashburn, VP-Communications, Legislative & External Affairs
Robert Sellers, VP – IT Infrastructure and Operations
Bruce Meeks, Inspector General
Mitch Brockbank, Director – IT Risk and Security
Spencer Kraemer, Director – Purchasing

**Audit Committee**
Juan Cocuy, Citizens Audit Committee Chairman
Bette Brown, Citizens Audit Committee Member
Jim Henderson, Citizens Audit Committee Member

**Following Audit Committee Distribution**
The Honorable Rick Scott, Governor
The Honorable Jeff Atwater, Chief Financial Officer
The Honorable Pam Bondi, Attorney General
The Honorable Adam Putnam, Commissioner of Agriculture
The Honorable Andy Gardiner, President of the Senate
The Honorable Steve Crisafulli, Speaker of the House of Representatives

Dixon, Hughes, Goodman LLP

**Audit Performed By**

<table>
<thead>
<tr>
<th>Auditor in Charge</th>
<th>Kirk Elmore, Senior Auditor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Director</td>
<td>Karen Wittlinger, IT Audit Director</td>
</tr>
</tbody>
</table>

**Under the Direction of**

Joe Martins
Chief of Internal Audit