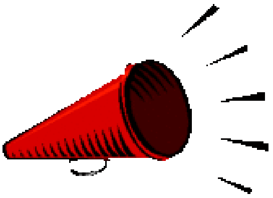

Assistance and Guidance Report

CITY OF TALLAHASSEE
OFFICE OF THE CITY AUDITOR

T. Bert Fletcher, CPA, CGMA
City Auditor

Cloud Computing

Report #1707

April 18, 2017

Introduction

The purpose of this report is to provide City departments and offices guidance and information on best practices for cloud computing activities and environments. The guidance and best practices information will provide City departments and offices a means to assess controls and processes regarding the selection and implementation of those cloud activities and environments.

Background

"Cloud computing" can be defined as the practice of using a facility (data center) physically located outside an entity's internally-managed network to house (host) the entity's information technology resources, to include data and software applications. Under this approach, the entity (e.g., the City) accesses its data and applications through an internet connection and web browser. The cloud host's data center consists of the building and related infrastructure that house the computer servers containing the entity's data and applications. The data center may be located anywhere: across town, in a different city, state, country, or continent, etc.

An entity electing to use a cloud environment pays the cloud host and, if also used, a separate cloud service manager for those services. The fees are typically based on the number of staff (e.g., City staff) that access and use the data, the amount of data stored and transmitted between those users and the cloud host's data center, and the specific cloud environment and services used. There are four specific industry-defined cloud environments: public clouds, private clouds, community clouds, and hybrid clouds.

Under a public cloud environment multiple entities (e.g., private companies, governments, citizens) share the use of the cloud host's data center (i.e., the cloud host has multiple customers using the same data center). Because multiple entities share the data center and related infrastructure (buildings, environmental controls, backup power supply, computer servers, etc.) the cost of using a public cloud is typically the least expensive cloud environment. Within a public cloud environment, virtual networks are created and used to isolate each participating entity's data and applications from that of the other participating entities (customers).

Under a private cloud environment one entity is the sole (only) user or customer of the cloud host's data center. Private clouds may be owned and managed by the user entity, or owned by a third party and leased to the user entity. Private clouds are typically the most expensive cloud environment because the underlying infrastructure expense for establishing and operating private clouds is not shared with other users.

Under a community cloud environment entities that follow the same security regulations share a cloud. For example, hospitals may share a community cloud because they are each bound by the same health care privacy laws. Similarly, municipalities with police departments could potentially share a community cloud established for record systems that contain confidential data. Like a public cloud, each entity's data is isolated from the other users through the use of virtual networks. The advantage of a community cloud is the cloud host can customize its cloud environment for the needs of one particular business sector. Compared to a public cloud, that specific industry customization by the cloud host typically saves the user entity time and potentially money, as the user entity does not have to establish unique industry-related security measures for its portion of the cloud.

Under a hybrid cloud environment two or more of the previously described cloud types are combined by an entity, such as when an entity houses some data (e.g., financial information) in a public cloud and other data (e.g., personnel records) in a private cloud.

Similar to cloud environments, there are different categories of cloud-based services, to include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS can be defined as the circumstance in which an entity (e.g., the City), in essence, "rents" servers and space (capacity) within a cloud host's data center to process and manage its data. The cloud host does not manage or process the entity's data. The entity continues to process its data through the established internet connection and web browser.

PaaS can be defined as the circumstance in which a customer (user entity) accesses and uses a computer operating system installed in a cloud provider's data center. In other words, instead of installing that operating system on its own computers, the customer pays to use a system installed in the cloud. PaaS is typically used in circumstances where entities need to design and develop specialized software applications through an appropriate operating system that is not installed on its own computers. Entities that use PaaS to develop such software applications also may use the PaaS host to host and run that software.

SaaS can be defined as the circumstance in which a customer (user entity) acquires the rights to use a unique software application (product) from a vendor, and that unique software application is housed in a data center owned or controlled by the vendor. The software application is accessed by the user entity's employees on their computers through a web browser. An example of this service is Kronos, the City's time and attendance system.

The determination as to which cloud environment and cloud-based services are appropriate depends on the circumstances and services needed by the user entity. For each situation in which a cloud environment may be appropriate, management should review the applicable circumstances and consider potential efficiencies that may be realized, and costs that likely may be incurred, as part of the decision making process.

Standards Followed for this Assistance and Guidance Report

The information for this assistance and guidance report was based on the audit work conducted in our Audit of the Cloud Migration and Upgrade to PeopleSoft Systems, Report #1706, issued April 7, 2017. We conducted that audit in accordance with the International Standards for the Professional Practice of Internal Auditing and Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

Cloud Best Practices

The following table provides best practices obtained from our research and review of information technology and audit reports of other entities, authoritative guides and reports (i.e., white papers), periodicals, and other industry materials; as well as from our prior audit experience. Topics addressed by the identified best practices include data and/or system security, privacy, protection, and access; environmental controls; backup and disaster recovery; and system performance and availability.

Table 1 – Best Practices for Migrating to a Cloud Environment

A. Transition/Migration Practices

1. During the conceptual phase of a cloud project and/or a cloud environment purchase, an organization’s management and information technology (IT) department should be consulted as to what specific cloud environment and cloud-based services are appropriate. In determining whether the project should be completed and/or the purchase made, a cost-benefit analysis should be completed as to the efficiencies that are anticipated and the related initial and ongoing costs that will likely be incurred.
2. An organization’s IT department should be consulted during the planning and vendor selection phases of any cloud migration or acquisition efforts for the purpose of evaluating the technological impact to the organization, the technology risks to which the organization will be exposed, and the controls that should be implemented in the event the cloud services are acquired and used.
3. Prior to executing a contract, and annually thereafter, organizations should obtain and review appropriate independent IT security audit reports of the cloud service provider. The underlying audit should be based on standards set forth by the American Institute of Certified Public Accountants. A Service Organization Control (SOC) 2 Type II Report is preferred; however, a SOC 2 Type I report may be appropriate in some circumstances. In other circumstances an equivalent type report may be acceptable. The organization’s IT department should be consulted regarding which report type is appropriate given the nature of the transition. Appropriate actions should be taken based on the information identified in those audit reports.
4. A cloud environment (e.g., servers, network infrastructure, communication capacity, etc.) should be tested extensively prior to transitioning to a cloud environment. Such testing should include key users completing actions they normally would perform in the course of their work for the purpose of ensuring those tasks can be accomplished appropriately. As appropriate, load testing should be a part of these tests to ensure the environment is adequate to meet the volume of activity expected during normal operations.
5. Prior to transitioning to a cloud environment, organizations should ensure there is sufficient bandwidth to successfully operate in that environment.
6. The organization should establish a change management strategy to govern the cloud migration process and system upgrades within the cloud environment.
7. Organization employees should be trained on system changes necessitated by the migration to the cloud environment.
8. A formal exit plan should be established to provide a smooth transition when cloud based applications and data are transitioned from one cloud service provider to another, or transitioned (back) to an “in-house” (internal) environment.

B. Contract Provision Practices

9. Data and application ownership should be stipulated in contracts established with cloud hosting service providers.
10. Contracts for cloud services should establish cloud availability guidelines defining what percentage of time (e.g., 99.999%) the cloud environment is guaranteed to be available to the organization.
11. An organization’s risk management team should be consulted prior to executing a contract with a vendor to review and determine if the proposed vendor’s insurance coverage is adequate given the types of risk associated with the particular cloud service being acquired.
12. The organization’s contract with the cloud service provider should include language stating the provider will "defend and hold harmless" the organization in the event of unauthorized access to the organization’s data and applications, such as a breach.
13. The organization’s contract with the cloud service provider should include the organization’s right to audit the provider’s processes, controls, and actions relevant to the organization.

C. Operations and Security Practices

14. Organizations should have and follow a formal and documented cloud policy when operating in a cloud environment.

15. The cloud service provider should be required to notify the organization in the event the provider no longer maintains relevant industry certifications.

16. The organization should have the right to allow, deny, or delay system upgrades or changes to the data center's servers housing the organization's data and applications.

17. Data in the cloud should be backed up and protected in accordance with organizational standards.

18. A Business Continuity/Disaster Recovery Plan (DR Plan) should be developed for the cloud environment.

19. The organization should ensure the cloud service provider has an adequate plan to protect the organization's data and applications in the event of a man-made or natural disaster.

20. The organization should evaluate the cloud service provider's planned downtime procedures for their impact on the organization's operations.

21. Organizations using cloud services should be aware of the information retained by the cloud vendor regarding the organization's specific IT network and activities, such as data volumes or locations of users that access the cloud-based services. Additionally, organizations should be made aware of the circumstances in which that information is made available to third parties by the cloud host.

22. Appropriate measures should be taken to prevent unauthorized intrusion and malware in cloud based data centers.

23. Cloud service providers should, on a regular and periodic basis, conduct (or have conducted) testing of the security of their data centers. Such tests should include, at a minimum, vulnerability scans and network penetration testing. Appropriate action should be taken based on the results of those scans and tests.

24. Organizations should ensure data and applications hosted in a cloud environment are stored in data centers physically located within the contiguous United States.

25. To protect its integrity, data in a cloud environment should be encrypted at all times (i.e., while stored in a data center and while being transmitted to and from the data center).

26. Organizations should know who has administrative level access to data and applications in their cloud environments.

27. To ensure proper management and oversight, the organization should verify the cloud service provider has administrator access to the entire data center.

28. Organizations should analyze the cloud service provider's formal information security policies to ensure up-to-date security technology and processes are being used, and to also ensure security procedures for the cloud environment meet or exceed the organization's standards.

29. Organizations should have a process or contractual provisions to block third party vendor access to the cloud hosted systems and data when that access is no longer needed.

30. Organizations should ensure the cloud service provider has a reasonable process for handling distributed denial of service (DDoS) attacks and data breaches, and require the cloud provider to notify the organization in the event of any unauthorized breach within the data center housing the organization's data and applications.

31. The organization should determine how the cloud service provider controls physical access to its data center, including the server room.

32. The organization should ensure the cloud service provider requires visitors to sign in and be escorted at all times they are inside the provider's data center.

33. The organization should ensure the cloud service provider requires data center employees to display identification badges while at work.
34. The organization should verify secure areas of the cloud service provider's data center are monitored by closed circuit television.
35. The organization should verify the cloud service provider performs adequate background checks on employees granted access to the provider's data center.
36. The organization should verify its data and applications are properly segregated within the data center from that of other users (customers).
37. Organizations should require the use of geo-blocking measures to preclude remote computers located outside of a defined geographical area from accessing the cloud-based systems and data.

Conclusion and Recommendation

Cloud computing can benefit the City through the provision of additional and/or more efficient information technology resources for the operation of City software applications. However, there are inherent risks associated with transitioning (migrating) to a cloud environment due, in part, to the partial relinquishment of control over City data and applications to a third party (cloud host). Accordingly, prior to transitioning to a specific cloud environment or product, appropriate analyses and assessments should be performed by knowledgeable staff to determine if the cloud environment and/or product are appropriate under the circumstances.

To assist management in the conduct of such analyses and assessments, we recommend the checklist included as Appendix A be completed by City departments or offices that are transitioning (migrating), or considering a transition, of an applicable City system to a cloud environment or product. Applicable systems include, for example, City enterprise systems, critical departmental systems, or other systems that are significant in regard to City operations. This checklist can also be used by management as a tool for the periodic review and evaluation of ongoing cloud hosted activities.

Copies of this Assistance and Guidance Report #1707, or Audit of the Cloud Migration and Upgrade to PeopleSoft Systems Report #1706, may be obtained from the City Auditor's web site (http://www.talgov.com/transparency/auditing-auditreports.aspx), or via request by telephone (850-891-8397), by FAX (850-891-0912), by mail or in person (City Auditor, 300 S. Adams Street, Mail Box A-22, Tallahassee, FL 32301-1731), or by e-mail (auditors@talgov.com).

This Assistance and Guidance Report was prepared by:
Patrick A. Cowen, CPA, CISA, CIA, Senior IT Auditor
T. Bert Fletcher, CPA, CGMA, City Auditor

Appendix A – Checklist for Migrating to a Cloud Environment

	Yes	**No**	**N/A**
A. Transition/Migration Practices			
1. During the conceptual phase of this cloud migration and/or cloud environment purchase:			
a. Has the City's Technology and Innovations Department (T&I) been consulted as to what specific cloud environment (public, etc.) and cloud-based services (IaaS, etc.) are appropriate?	□	□	□
b. Has a cost-benefit analysis been completed for this migration that compares the cost of using or staying within the City's internal network versus the initial and ongoing costs of moving to the cloud?	□	□	□
c. Did that cost-benefit analysis show this cloud migration would be more efficient than staying within the City's internal network?	□	□	□
Comments or explanation for answers:			
2. Has T&I evaluated from a technology standpoint the impact to City operations, the related risks, and the related controls necessary for this particular cloud service?	□	□	□
Comments or explanation for answers:			
3. Prior to selecting and contracting with a cloud vendor:			
a. Was a current independent IT security audit report for the cloud vendor obtained and reviewed by appropriate City staff? *This report should be obtained and analyzed annually thereafter.*	□	□	□
b. Was the underlying audit based on standards set forth by the American Institute of Certified Public Accountants (e.g., Service Organization Control [SOC] 2 Type II Report)?	□	□	□
c. Was there a satisfactory resolution to any issues disclosed in the security audit report that should be considered and/or resolved prior to the City using the vendor?	□	□	□
Comments or explanation for answers:			
4. Prior to transitioning to a cloud environment:			
a. Was extensive and appropriate testing of the cloud environment conducted?	□	□	□
b. Was load testing performed?	□	□	□
c. Did the test results show the cloud environment would work properly at the expected levels and volumes of City activity?	□	□	□
Comments or explanation for answers:			

	Yes	No	N/A
5. Prior to transitioning to a cloud environment, was a determination made that there is sufficient bandwidth available to successfully operate in that cloud environment?	□	□	□
Comments or explanation for answers:			
6. Was the City's change management policy followed during the cloud migration and implementation process?	□	□	□
Comments or explanation for answers:			
7. Were City employees trained on system changes necessitated by the migration to the cloud environment?	□	□	□
Comments or explanation for answers:			
8. Has a formal documented exit plan been established to provide a smooth transition in the event data and cloud based applications are transitioned from one cloud service provider to another, or transitioned (back) to an "in-house" (internal) environment?	□	□	□
Comments or explanation for answers:			
B. Contract Provision Practices			
9. Does the contract for this cloud service stipulate the City retains ownership of the data and application being used in the cloud environment?	□	□	□
Comments or explanation for answers:			
10. Does the cloud service contract establish acceptable availability guidelines defining what percentage of time (e.g., 99.999%) the cloud environment is guaranteed to be available to the City?	□	□	□
Comments or explanation for answers:			

	Yes	**No**	**N/A**
11. Prior to executing a contract, was the City’s risk management team consulted to review and determine if the proposed vendor’s insurance coverage is adequate given the types of risk associated with the particular cloud service being acquired?	□	□	□
Comments or explanation for answers:			
12. Does the contract with the cloud service provider include language stating the provider will "defend and hold harmless" the City in the event of unauthorized access to the organization’s data and applications, such as a breach?	□	□	□
Comments or explanation for answers:			
13. Does the contract with the cloud service provider include the City’s right to audit the provider’s processes, controls, and actions relevant to the City?	□	□	□
Comments or explanation for answers:			
C. **Operations and Security Practices** (*Some of the following checklist items [questions] may be completed [answered] based on a review of the independent IT security audit report addressed in checklist item A.3)*			
14. Did this implementation follow appropriate provisions of the City’s cloud policy? *Note: as of the date of this assistance and guidance report, the City’s Technology and Innovations Department is in the process of developing a formal cloud policy*.	□	□	□
Comments or explanation for answers:			
15. Is the cloud service provider required to notify the City in the event the provider no longer maintains relevant industry certifications?	□	□	□
Comments or explanation for answers:			
16. Does the City have the right to deny or delay system upgrades or changes to data center servers housing the City’s data and applications?	□	□	□
Comments or explanation for answers:			

	Yes	No	N/A
17. Is a plan in place to ensure data being migrated to the cloud is backed up in accordance with the City's information technology (IT) security guidelines?	□	□	□
Comments or explanation for answers:			
18. Is a Business Continuity/Disaster Recovery Plan (DR Plan) in place for this cloud service?	□	□	□
Comments or explanation for answers:			
19. Does the cloud service provider have an adequate plan to protect the City's data and applications in the event of a man-made or natural disaster?	□	□	□
Comments or explanation for answers:			
20. Has the City evaluated the cloud service provider's planned downtime procedures for the impact on City operations? Is that impact acceptable?	□	□	□
Comments or explanation for answers:			
21. The cloud service provider inherently has access to certain information about the City's network and activities:			
a. Is the City aware of and acceptable to what information is being retained by the cloud vendor regarding the City's specific IT network and activities, such as data volumes or locations of users that access the cloud-based services?	□	□	□
b. Is the City aware of and acceptable to the circumstances in which that information is made available to third parties by the cloud vendor?	□	□	□
Comments or explanation for answers:			
22. Are appropriate measures being taken to prevent unauthorized intrusion and malware in data centers used for this particular cloud service?	□	□	□
Comments or explanation for answers:			

	Yes	No	N/A
23. Does the cloud service provider conduct (or have conducted) a regular and periodic testing of the security of their data centers (e.g., vulnerability scans and network penetration tests), and has the cloud service provider taken appropriate action based on the results of those tests?	□	□	□
Comments or explanation for answers:			
24. Are the hosted data and applications stored in data centers physically located within the contiguous United States?	□	□	□
Comments or explanation for answers:			
25. Is the data being housed in the cloud environment encrypted at all times (i.e., while stored and while in transmission)?	□	□	□
Comments or explanation for answers:			
26. In determining who has access to the City's data and applications maintained in the cloud:			
a. Does the City have a record of individuals with administrative level access to the City's data and applications within the cloud environment?	□	□	□
b. Have non-City individuals with administrative access been required to complete a "Compliance Statement" to attest they will abide by appropriate City policies and procedures, as required in Administrative Policies and Procedures #809?	□	□	□
Comments or explanation for answers:			
27. To ensure proper management and oversight, has the City verified the cloud service provider has administrator access to the entire data center?	□	□	□
Comments or explanation for answers:			
28. Has the cloud service provider's formal information security policies been analyzed by T&I staff to ensure up-to-date security technology and processes are being used, and to also ensure security procedures for the cloud environment meet the City's IT security guidelines?	□	□	□
Comments or explanation for answers:			

	Yes	No	N/A
29. Does the City have a process in place blocking third party vendor access to the cloud hosted systems and data when that access is no longer needed?	□	□	□
Comments or explanation for answers:			
30. In evaluating how the cloud service provider protects the City's cloud environment:			
a. Has the City determined the cloud service provider has an acceptable process for handling distributed denial of service (DDoS) attacks and data breaches?	□	□	□
b. Does the City require the cloud service provider to promptly notify the City in the event of an unauthorized breach within data centers housing the City's data and applications?	□	□	□
Comments or explanation for answers:			
31. Does the cloud service provider control physical access to its data center, including the server room?	□	□	□
Comments or explanation for answers:			
32. Does the cloud service provider require visitors to sign in and be escorted at all times they are inside the provider's data center?	□	□	□
Comments or explanation for answers:			
33. Does the cloud service provider require data center employees to display identification badges while at work?	□	□	□
Comments or explanation for answers:			
34. Does the cloud service provider monitor its data centers through closed circuit television?	□	□	□
Comments or explanation for answers:			

	Yes	No	N/A
35. Does the cloud service provider perform adequate background checks on employees granted access to its data center?	□	□	□
Comments or explanation for answers:			
36. Does the cloud service provider properly segregate the City’s data and applications within the data center from that of other users (customers)?	□	□	□
Comments or explanation for answers:			
37. Are geo-blocking measures being used to preclude computers located outside of a defined geographical area from accessing the cloud-based systems and data?	□	□	□
Comments or explanation for answers:			