MAYOR LINDA GORTON

LEXINGTON

BRUCE SAHLI
DIRECTOR
OFFICE OF INTERNAL AUDIT

INTERNAL AUDIT REPORT

DATE: September 11, 2020

TO: Linda Gorton, Mayor

CC: Sally Hamilton, Chief Administrative Officer
Glenn Brown, Deputy Chief Administrative Officer
Aldona Valicenti, Chief Information Officer
Chad Cottle, Deputy Chief Information Officer
William O'Mara, Commissioner of Finance & Administration
Mike Nugent, Director of Technical Services
Todd Slatin, Director of Purchasing
Phillip Stiefel, Director of Enterprise Solutions
Phyllis Cooper, Director of Accounting
Susan Straub, Communications Director
Urban County Council
Internal Audit Board

FROM: Bruce Sahli, CIA, CFE, Director of Internal Audit
Jim Quinn, CIA, CISA, Internal Auditor

RE: Cloud Computing Governance & Controls Audit

Background

The cloud computing model is a method of procuring and deploying information technology (IT) resources and applications using only a network connection, which is often done by accessing data centers using wide area networking or internet connectivity. According to the National Institute of Standards and Technology (NIST),

cloud computing is "a model for enabling 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."

The NIST definition lists five essential characteristics and benefits of cloud computing, including on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. NIST also lists three cloud service models which organizations can typically utilize including software (SaaS, software as a service), platform (PaaS, platform as a service) and infrastructure (IaaS, infrastructure as a service).

Primary uses of cloud computing within the Lexington-Fayette Urban County Government are for software as a service (SaaS) and/or infrastructure as a service (IaaS), in which applications, services, and storage are hosted in a cloud service provider (CSP) data center and where LFUCG data is processed and/or stored. Like many organizations, LFUCG has begun within the last few years moving more of its computer applications, systems, and services to the cloud.

Scope and Objectives

The general control objectives for the audit were to provide reasonable assurance that:

- Cloud computing governance and security policies and procedures have been established and are being followed
- A comprehensive inventory of all LFUCG cloud services and applications exists and these services and applications are being sufficiently governed and monitored by the Department of Information Technology
- Contracts and Service Level Agreements (SLAs) with cloud service providers (CSPs) and managed service providers (MSPs) sufficiently define security and performance requirements, and these requirements are being sufficiently monitored and managed by the Department of Information Technology and by other responsible LFUCG Division and Department personnel

Audit results are based on observations, inquiries, transaction examinations, and the examination of other audit evidence and provide reasonable, but not absolute, assurance controls are in place and effective. In addition, effective controls in place

during an audit may subsequently become ineffective as a result of technology changes or reduced standards of performance on the part of management.

The period of review for the audit included transactions from June 2014 through March 2020.

Statement of Auditing Standards

We conducted our audit in accordance with the International Standards for the Professional Practice of Internal Auditing. Those standards require that we plan and perform the audit to afford a reasonable basis for our judgments and conclusions regarding the organization, program, activity or function under audit. An audit also includes assessments of applicable internal controls and compliance with requirements of laws and regulations when necessary to satisfy the audit objectives. We believe that our audit provides a reasonable basis for our conclusions.

Audit Opinion

In our opinion, the controls and procedures provided reasonable assurance that the general control objectives were partially being met. Opportunities to improve controls are included in the Summary of Audit Findings.

Priority Rating Process

To assist management in its evaluation, the findings have been assigned a qualitative assessment of the need for corrective action. Each item is assessed a high, moderate, or low priority as follows:

> High - Represents a finding requiring immediate action by management to mitigate risks and/or costs associated with the process being audited.
>
> Moderate – Represents a finding requiring timely action by management to mitigate risks and/or costs associated with the process being audited.

Low - Represents a finding for consideration by management for correction or implementation associated with the process being audited.

SUMMARY OF AUDIT FINDINGS

Finding #1: No Formal Policies and Procedures Exist To Require Department of Information Technology Involvement Before Cloud Services Are Acquired By LFUCG Business Units
Priority Rating: High

Condition:
The use of cloud services for business functions is growing across LFUCG. To effectively evaluate IT internal controls and processes related to the acquisition and implementation of cloud services, we used the Control Objectives for Information and Related Technology (COBIT) framework created by the Information Systems Audit and Control Association (ISACA) for IT governance and management.

Process D1 of this framework, Define and Manage Service Levels states, "Effective communication between IT management and business customers regarding services required is enabled by a documented definition of an agreement on IT services and service levels… This process enables alignment between IT services and the related business requirements". Process D2, Manage Third-Party Services requires, "the need to ensure that services provided by third parties meet business requirements."

Our inquiry with Department of Information Technology management and LFUCG Departments and Divisions using cloud service applications, along with a review of a sample of current cloud service applications maintained and managed by LFUCG, determined that there are no policies or procedures requiring collaboration between the Department of Information Technology and LFUCG Departments or Divisions transitioning to cloud service applications prior to these cloud services being obtained. We also noted there were no comprehensive IT policies, procedures, or guidelines available to instruct Department or Division business units transitioning to cloud service applications in the acquisition, use, and management of cloud services, or to address the need for pre-acquisition information security risk assessments, or addressing vendor management once a signed agreement is in place.

Effect:
The absence of formal policies and procedures governing the acquisition and management of cloud computing resources with third-party vendors by various LFUCG Departments or Divisions could lead to substandard vendor selection and performance and increased IT security risks.

Recommendation:
Department of Information Technology management should develop formal written policies and procedures which will authorize them to consult and advise other LFUCG Departments and Divisions prior to the approval, acquisition, and implementation of any cloud-based services to ensure that the services are consistent with stated LFUCG business objectives and that IT performance standards and data security risks are sufficiently addressed. This consult and advise process should also be supported by the Division of Purchasing by requiring Departments or Divisions to document on the Bid/RFP/Formal Quote Request Form that they have consulted with the Department of Information Technology regarding any cloud-based services they wish to purchase.

Consistent with COBIT best practices, the Department of Information Technology may want to consider creating a checklist/template to aid in consistently evaluating cloud services, including application security, availability capabilities, and any associated risks.

Director of Purchasing Response:
The Division of Purchasing has updated the bid request form to include a sign-off by the Chief Information Officer for all software, hardware and cloud related bid/RFP requests. This form is automatically sent to users requesting new bids or RFPs for all goods and services.

Commissioner of Finance & Administration Response:
I concur with the Director of Purchasing's response.

Chief Information Officer Response:
The Department of Information Technology has worked with the Division of Purchasing and the Director has confirmed (in writing) that an IT signoff is required for the purchase (or lease) of IT equipment, software, cloud services, etc. We will create a CIO policy that references the Division of Purchasing's standards and procedures. Additionally, we will ensure that it covers SLAs as per finding #3 in this audit document.

Chief Administrative Officer Response:
I concur with the Chief Information Officer's response.

Finding #2: No Comprehensive Inventory of LFUCG Cloud Services and Cloud Service Providers Exists
Priority Rating: High

Condition:
COBIT Process DS2.1 Identification of All Supplier Relationships, states organizations should, "Identify all supplier services, and categorize them according to supplier type, significance, and criticality" and, "Maintain formal documentation of technical and organizational relationships covering the roles and responsibilities, goals, expected deliverables, and credentials of representatives of these suppliers".

Department of Information Technology management could not provide a complete list of all cloud computing resources utilized by the various LFUCG Departments or Divisions. Department of Information Technology management was able to provide an unofficial list of 22 different cloud computing services they manage and that are part of their current budget, but stated this did not include all cloud services being provided to the LFUCG Departments and Divisions.

Effect:
Without a comprehensive inventory of all LFUCG cloud services and cloud services providers, the LFUCG is not able to determine whether all cloud related IT performance standards and data security risks are sufficiently identified, assessed, and managed.

Recommendation:
Department of Information Technology management should develop a comprehensive inventory of LFUCG cloud services and cloud service providers consistent with the recommendations contained in COBIT Process DS2.1.

Chief Information Officer Response:
We concur with this finding and will compile and maintain a formal inventory of cloud services. Additionally, a staff member will be assigned to maintain the inventory and manage the review process. This review process will be noted in the forthcoming policy as outlined in finding #1.

Chief Administrative Officer Response:
I concur with the Chief Information Officer's response.

Finding #3: Establishment and Monitoring of Service Level Agreements Should Be Improved
Priority Rating: High

Condition:
In using cloud infrastructures and cloud data centers, the customer necessarily cedes control and governance to the cloud service provider (CSP). Therefore, it is important for the customer to establish a comprehensive Service Level Agreement (SLA) with the cloud service provider which aligns with and supports its business requirements, is accepted by the service provider, can be monitored for service performance, and addresses system security risks.

COBIT DS1.3 Service Level Agreements recommends, "Define and agree to SLAs for all critical IT services based on customer requirements and IT capabilities…Consider items such as availability, reliability, performance, capacity for growth, levels of support, continuity planning, security and demand constraints." In addition, COBIT DS2.4 Supplier Performance Monitoring states, "Establish a process to monitor service delivery to ensure that the supplier is meeting current business requirements and continuing to adhere to the contract agreements and SLAs, and that performance is competitive with alternative suppliers and market conditions." Furthermore, COBIT DS1.6 Review of Service Level Agreements and Contracts states, "Regularly review SLA's and underpinning contracts…to ensure that they are effective and up-to-date and that changes in requirements have been taken into account."

Based on the COBIT standards quoted above, Department of Information Technology management should be actively involved with each Department or Division business unit in establishing SLAs with cloud service providers to ensure all LFUCG customer requirements and IT capabilities are properly addressed. The SLAs should be examined for the inclusion of measurable metrics to be provided by the cloud service providers that will allow for appropriate oversight and early detection of unacceptable vendor performance and any security risks which may be introduced.

We selected five significant LFUCG cloud service applications/systems for review. We attempted to obtain the most recent Service Level Agreements (SLAs) LFUCG has in

force with either the managed service provider (MSP) or cloud service provider (CSP) for these systems. We found that two of the systems selected had sufficient SLA agreements in place with their third-party providers with detailed provisions for defined service and support levels, metrics, and reporting. However, the SLAs for two other systems and their providers had expired without being replaced, and the conditions contained therein were insufficient to provide satisfactory support and reporting services. We were unable to obtain an SLA for one of the systems and its cloud service provider. We also noted that a formal process for the Department of Information Technology to work with LFUCG business units to establish and evaluate SLAs for cloud services prior to implementation was generally deficient.

Effect:
If comprehensive cloud service SLAs are not properly established and the vendor service is not properly monitored for SLA compliance, inadequate cloud services and support could occur, resulting in LFUCG cloud service business needs not being met and IT security risks being introduced into the LFUCG system network.

Recommendation:
The two expired Service Level Agreements should be renewed and the conditions contained therein should be amended to provide satisfactory support and reporting services. A copy of the unavailable Service Level Agreement should be obtained from the vendor and kept on file in the Division business unit receiving this vendor's cloud service. The Department of Information Technology should keep a backup copy of this Agreement.

The Department of Information Technology should establish a formal process to collaborate with all LFUCG Departments and Divisions that obtain new cloud-based services to ensure that the SLAs entered into with cloud service providers clearly address business requirements, needed services, and all IT security requirements. This process should always occur before the cloud-based services are procured. As a best practice based on the COBIT 5 framework, Department of Information Technology management should consider creating a list of controls/evaluation criteria (essentially a risk assessment) to assist LFUCG Departments and Divisions in their decision making process when considering the procurement of cloud-based services.

The Department of Information Technology should also develop guidelines that define roles and responsibilities within Departments and Divisions receiving cloud-based services to ensure that service levels specified in the SLAs are consistently provided

once the cloud service is implemented. The Department of Information Technology should also work with Department and Division business units with cloud services in reviewing their respective SLA's at least annually to provide reasonable assurance the SLAs are up-to-date, any changes in business process requirements are identified, and any necessary adjustments are made to the SLAs when the opportunity to re-negotiate them occurs.

Chief Information Officer Response:
We concur and will work with Departments and Divisions to review and encourage them to update their SLAs. A Computer Systems Manager (or their designee) will be assigned the role of acquiring, tracking and managing SLAs for all third party systems. This will tie back in to finding #1 and we will provide assistance for this process to the business units.

Chief Administrative Officer Response:
I concur with the Chief Information Officer's response.

Finding #4: Third-Party Control Assessment Reports From Cloud Service Providers Not Obtained and Reviewed
Priority Rating: Moderate

Condition:
We determined that most LFUCG Departments and Divisions receiving cloud-based services were not obtaining SOC 2 reports from their cloud service providers. SOC 2 reports address a cloud service provider's operations and compliance controls as set forth in the American Institute of Certified Public Accountants (AICPA) Trust Services Criteria, which includes security, availability, processing integrity, confidentiality, and privacy.

Effect:
By not reviewing all cloud service provider SOC 2 reports on an annual basis, LFUCG relinquishes an opportunity to possibly become aware of otherwise unknown cloud-based IT security risks.

Recommendation:
SOC 2 reports for all LFUCG cloud service providers should be obtained and reviewed annually by knowledgeable Department of Information Technology personnel. Any IT

concerns noted therein should be discussed with the management of Department or Division business process owners responsible for the oversight of their respective cloud based services to determine how to address these concerns with the third party cloud service provider.

Chief Information Officer Response:

IT will request that each business unit contact their cloud services provider and ask for a SOC 2, Type 2. It should be noted that IT has requested these in the past and some companies either don't have them or will not share them publicly. Potential vendors may be reluctant to distribute SOC 2 Type 2 reports to non-clients or without some form of NDA. In these situations, a SOC 3 report should be requested. SOC 3 provides an overview of security, availability, process integrity, confidentiality, and privacy which is normally freely distributable. The request for a SOC report should be part of the vendor selection process, and it may impact vendor selection.

Chief Administrative Officer Response:

I concur with the Chief Information Officer's response.