OFFICE OF THE CITY CONTROLLER

HOUSTON INFORMATION TECHNOLOGY SERVICES
CLOUD GOVERNANCE PERFORMANCE AUDIT

Chris B. Brown, City Controller

Courtney E. Smith, City Auditor

Report No. 2018-09

OFFICE OF THE CITY CONTROLLER
CITY OF HOUSTON
TEXAS

CHRIS B. BROWN

June 6, 2018

The Honorable Sylvester Turner, Mayor
City of Houston, Texas

SUBJECT: REPORT #2018-09
HOUSTON INFORMATION TECHNOLOGY SERVICES – CLOUD GOVERNANCE PERFORMANCE AUDIT

Mayor Turner:

The Office of the City Controller's Audit Division contracted the professional services of Experis to complete a performance audit of cloud governance as managed by the Houston Information Technology Services (HITS) Department. The "cloud" is a term referring to accessing computer, information technology (IT), and software applications through a network connection, which is often done by accessing data centers using wide area networking or internet connectivity.

HITS is under new leadership and is in a state of transformation with the fundamental goal of providing solutions that serve, protect and enlighten the citizens of the City of Houston. The Department's mission is to be recognized as an innovative center of excellence focused on the continuous rapid delivery of high quality solutions to help transform the City of Houston into a digital city for all.

The primary audit objectives were to determine the existence and effectiveness of information technology governance policies regarding cloud applications.

The engagement scope period included relevant activities and processes in place from May through December 2017.

During the audit, we noted that the transformation of HITS has only been underway for a short span of time (13 months) however this activity has resulted in:

- Strategic direction on the implementation of efficient value-added solutions;
- Identification and development of core policies and procedures;
- Email migration to the cloud;
- Introduction of significant infrastructure enhancements and stability; and
- Focus on cybersecurity and threat mitigation.

We determined that of the seven controls reviewed, four had a maturity level categorized as "Developing", two of the controls reviewed had a maturity level categorized as "Initial" and one was categorized as "Defined". The report also documents exceptions including:

- There is no formal inventory of cloud services maintained by the City;
- No formal checklist exists to consistently review and evaluate the security capabilities of vendors nor a consistent process to review contracts and make risk decisions;

- The City does not have an Enterprise Risk Management (ERM) model, risk management process, or risk framework in place;
- For 5 of the 6 vendors reviewed, it was unclear who owns the data;
- All service level agreements reviewed did not contain clauses that ensure services in case of vendor acquisition or changes in management.

We would like to express our appreciation to the management and staff of the Houston Information Technology Services Department for their time and effort, responsiveness, and cooperation during this audit.

Respectfully submitted,

Chris B. Brown
City Controller

xc: Lisa Kent, Director, Houston Information Technology Services
City Council Members
Marvalette Hunter, Chief of Staff, Mayor's Office
Harry Hayes, Chief Operations Officer, Mayor's Office
Chris Mitchell, Deputy Director, Houston Information Technology Services
Shannan Nobles, Chief Deputy City Controller, Office of the City Controller
Courtney Smith, City Auditor, Office of the City Controller

June 5, 2018

Prepared for:

City of Houston

Houston Information Technology Services Department (HITS)
Cloud Application Governance Report

Experis™
Finance

Table of Contents

EXECUTIVE SUMMARY

Introduction

Experis has completed its Cloud Application Governance audit of Houston Information Technology Services. The audit considered the internal controls and process related to the governance of cloud based applications.

Background

The Houston Information Technology Services (HITS) Department

The Houston Information Technology Services (HITS) department provides enterprise IT services for the City of Houston (COH). These services include voice and network, cyber-security, email and communication platforms and shared enterprise applications that are used by all City employees. HITS approaches all solutions by evaluating what the short and long-term goals are of the customer and then seeks to find the most optimal solution. The portfolio of solutions/services contains a hybrid approach with both cloud and on-premise solutions.

Under new leadership and with renewed focus, the Houston Information Technology Services (HITS) Department is in a state of transformation with the fundamental goal of providing solutions that serve, protect and enlighten the citizens of the City of Houston. The mission of the department is to be recognized as an innovative center of excellence focused on the continuous rapid delivery of high quality solutions to help transform the City of Houston into a digital city for all. HITS is comprised of five (5) highly collaborative divisions including, Enterprise Infrastructure Services, Enterprise Applications Services, Radio Communication Services, Enterprise Cyber Security and a dedicated Project Management Office (PMO).

The transformation of HITS has been underway for 13 months and in this short span of time, the City of Houston is experiencing significant return on investment including:

- Strategic direction on the implementation of efficient, value added solutions
- Identification and development of core policies and procedures
- Email migration to the cloud
- Introduction of significant infrastructure enhancements and stability
- Focus on cybersecurity and threat mitigation

Audit Scope & Objectives

The Objective of this engagement was to assist the City of Houston to conduct a performance audit of Houston Information Technology Services – Cloud Application Governance, but not limited to the following:

- Determine the existence and effectiveness of information technology governance policies regarding cloud applications.

This engagement was done in two (2) parts. The goal of the preliminary planning phase ("Part One") was to gather information from appropriate sources necessary to develop a detailed Fieldwork Plan to ensure the accomplishment of the engagement goals, and provide deliverables to support the planning phase.

Procedures Performed

In order to obtain sufficient evidence to achieve engagement objectives and support our conclusions, we performed the following procedures:

Part One – Engagement and Planning

- Conducted opening conference
- Conducted initial interviews to determine roles, responsibilities, accountabilities, and expectations
- Requested population of cloud based and subscription vendors and contracts
- Obtained and reviewed applicable ordinances
- Obtained and reviewed applicable policies and procedures related to cloud application governance and/or cloud based service guidelines
- Identified the key internal controls related to inherent and residual risks
- Prepared an overall assessment that identified key components for a risk and controls heat map
- Developed a detailed work plan and staffing plan for Part Two and a budget for the City Auditor's review and approval.

Part Two – Fieldwork and Reporting

- Identified Cloud-Based and Subscription Type Service Vendors and Contracts
- Assessed controls surrounding vendor contract management (including Terms and Conditions and Expirations)
  - Scope of Services
  - Interface with client hardware and software
  - Consistency between City IT Controls and Vendor Terms/Conditions
  - Cyber-Security Responsibilities
  - Incident Reporting Standards
- Determined within contractors the extent of services provided by subcontractors
- Documented and tested client oversight and monitoring of cloud vendor performance against terms and conditions
- Determined application(s) existence, reliance level(s) for controls environment support, and testing
- Determined transactional population(s), selected sample(s), and tested compliance with policies, practices, and internal controls; maintained work papers, support for control failures
- Reported-out of observations- preliminary and final (with remediation plan and timeline)

Audit Methodology

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards and in conformance with the International Standards for the Professional Practice of Internal Auditing. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The scope of our work did not constitute an evaluation of HITS overall internal control structure. Management is responsible for establishing and maintaining a system of internal controls to ensure that City assets are safeguarded, financial activity is accurately reported and reliable, and management and employees are in compliance with laws, regulations, and policies and procedures. The objectives are to provide management with reasonable, but not absolute assurance that the controls are in place and effective.

Conclusions and Significant Issues

We believe that we have obtained sufficient and appropriate evidence to adequately support the conclusions provided below as required by professional auditing standards. The risk heat map illustrates our conclusions regarding inherent risk and the maturing level of the areas under review. For detailed findings, recommendations, management responses, comments and assessment of responses, see the "Detailed Findings, Recommendations, Management Responses, and Assessment of Responses" section of this report.

Risk Heat Map

Heat Map Definitions

Inherent Risk (IR):

The Heat Map on the following page summarizes the potential business risk/impact to the organization in the absence of any actions management might take to alter either the likelihood or impact.

As part of this review, COH's cloud application governance environment was evaluated for adequacy. An evaluation of the process is noted in each instance. Controls were evaluated as follows:

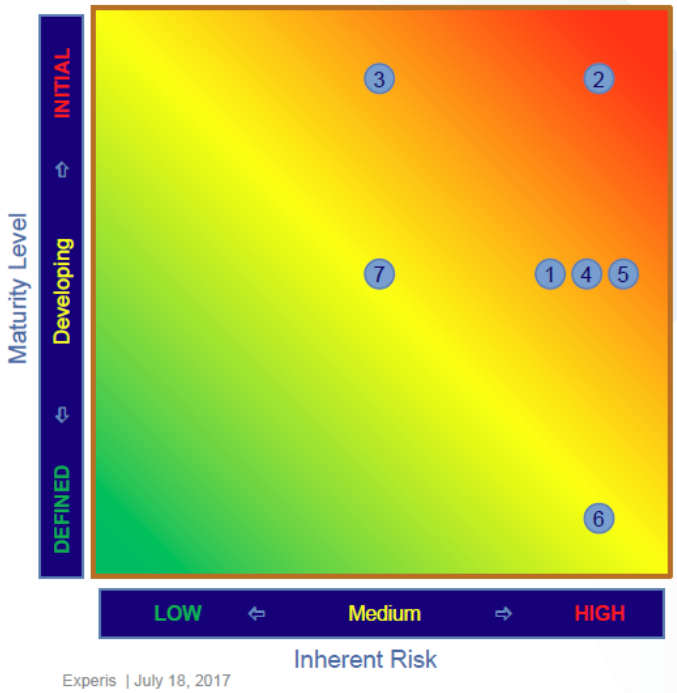
- **LOW** — Inherent Risk has a negligible impact, low probability
- **MEDIUM** — Inherent Risk has a significant impact, low probability or negligible impact, high probability
- **HIGH** — Inherent Risk has a significant impact and a high probability

Maturity Level (ML):

The Heat Map on the following page summarizes the business risk/impact to the organization, given the maturity of the existing control environment. The possibility that an event will occur and adversely affect the ability of the organization to achieve particular strategies and objectives. As it relates to financial and compliance goals, this could result in: loss of assets; poor business decisions; noncompliance/increased regulations, or public scandal.

- ● **DEFINED** — Processes are defined for the organization and are proactive
- △ **DEVELOPING** — Processes are characterized for specific projects and are often reactive
- ■ **INITIAL** — Process are unpredictable, poorly controlled and reactive

The Heat Map below summarizes the existence of controls established by management and the potential business impact based on the maturity level of cloud application governance controls observed during Part One - Planning & Scoping of the engagement.



	Controls	Current IR[1]	Current ML[2]
1.	Inventory - The COH has mechanisms in place to identify all providers and broker of cloud services with which it currently does business and all cloud deployments that exist across the enterprise	■	△
2.	Governance – The COH ensures that IT information security and business units actively participate in the governance and policy activities to align business objective and information security capabilities of the service provider with those of the COH	■	■
3.	Reporting – Both parties define the reporting relationship and responsibilities	△	■
4.	Risk Acceptance – Approved by a member of management with the authority to accept the risk on behalf of the COH and who understands the implications of the decision	■	△
5.	Risk Framework – A risk management framework and a maturity model have been implemented to quantify risk and assess the effectiveness of the risk model	■	△
6.	Business Continuity Disaster Recovery – The COH performs due diligence processes to ensure sustainability and compliance with regulatory requirements	■	●
7.	Regulatory Requirements – Data regulations are identified by compliance topic and are mapped to the regulator's requirements. Gaps are evaluated to determine if the cloud computing platform will invalidate or breach compliance requirements	△	△

Experis | July 18, 2017

[1]IR = Inherent Risk [2]ML = Maturity Level

7

Acknowledgement and Signatures

Experis Finance would like to thank the City of Houston City Auditor and Staff and the Houston Information Technology Services Department (HITS) for their responsiveness, cooperation, time and efforts, as well as their proactive approach to risk management throughout the course of this engagement.

Jeffrey Butler

_____

Director, Risk Advisory Services
Experis Finance

Detailed Findings, Recommendations, Management Responses, and Assessment of Responses

Finding # 1 – Governance of Cloud Computing Services - Inventory of Services from Cloud Providers
(Inherent Risk Rating = High)

Background: During Part One, we reviewed the areas within the COH managed by Houston Information Technology Services "HITS" to see if HITS has mechanisms in place to identify all providers and brokers of cloud services with which it currently does business and all cloud deployments that exist across the enterprise. The following review steps were conducted:

1. Determine if the COH maintains an inventory of all services provided via the cloud (including SaaS, PaaS, and IaaS).
2. Understand how inventory of cloud application is managed and updated.
3. Determine who the Business Owners are for each cloud application.
4. Determine that the business cannot procure cloud services without the involvement of information technology and information security.
5. Review applicable policies and procedures related to cloud application governance and/or cloud based service guidelines.

During Part One, 15 cloud vendors representing 22 applications were identified. Based on the inventory obtained in Part One, we initially selected 7 vendors representing 14 applications to conduct detailed testing and test compliance with policies, practices, and internal controls. One of the 7 vendors selected from the inventory list, ReadyHouston, was determined to be hosted on premise and not a cloud application. Therefore, 6 vendors representing 13 applications were used for the Part Two testing.

Findings: HITS maintains an unofficial inventory of all services provided via the cloud of which they are aware. There are other cloud services HITS is not aware of that are used by the City.

Recommendation: Creation of Cloud Inventory management procedures for HITS and communicate to other departments in COH.

Department Management Response: HITS will develop and implement a Cloud Computing Services Policy and distribute to department directors and CTOs. The policy will also officially establish a HITS managed cloud computing services governance committee to ensure cloud services requests are properly vetted prior to approval and implementation. Vetting responsibilities include but are not limited to business requirements, bandwidth consumption, information security/risk, maintenance and ownership. This approach will allow HITS to properly develop and maintain an accurate inventory of all cloud-based services across the City of Houston's information technology enterprise.

Responsible Party: Reenie Askew

Estimated Date of Completion: December 2019

Assessment of Response: The Management Response fully addresses issues identified in Finding #1.

Finding # 2 – Governance of Cloud Computing Services - Review of Provider Security Capabilities
(Inherent Risk Rating = High)

Background: During Part One, we reviewed the areas within the COH managed by Houston Information Technology Services "HITS" to see if HITS ensures that IT information security and business units actively participate in the governance and policy activities to align business objectives and information security capabilities of the service provider with those of the COH. The following review steps were conducted:

1. Determine if the IT, information security and key business functions have defined integrated governance framework and monitoring processes.
2. Determine if the IT and information security functions and key business units are actively involved in the establishment of service level agreements (SLAs) and contractual obligations.
3. Determine if the information security function has performed a gap analysis of the service provider's information security capabilities against the COH's information security policies and threat and vulnerabilities/IT risk emanating from the transition to cloud computing.
4. Determine if the cloud provider has identified control objectives for the provided services.

If IT and business units are not actively participating in the governance and policy activities, the following risks could materialize:

- Wrong technologies (i.e. cost, performance, features, compatibility) selected for implementation
- Business units not assuming accountability over those cloud areas for which it should (e.g. functional requirements, development priorities, opportunity assessment through new technologies)
- Inadequate support and services delivered by vendors, not in line with service level agreements
- Inadequate performance of cloud service provider in large-scale, long-term cloud arrangements

Findings: There is not a formal checklist to consistently review and evaluate the security capabilities of vendors. During our interviews, it was noted that HITS does review security capabilities of a cloud vendor. However, these procedures are not consistent across all providers. Also noted was that the areas of data control and ownership were not covered during contract negotiations or development & rollout.

Recommendation: As a best practice based on COBIT 5 framework, create a checklist/template for consistently evaluating application security and availability capabilities that includes data control, ownership, and survivability and is in line with HITS data classification, information architecture, information security architecture and risk tolerance.

Department Management Response: HITS will develop and implement a Cloud Computing Services Policy and distribute to department directors and CTOs. The policy will also officially establish a HITS managed cloud computing services governance committee to ensure cloud services requests are properly vetted prior to approval and implementation. Vetting responsibilities include but are not limited to business requirements, bandwidth consumption, information security/risk, maintenance and ownership. This approach will allow HITS to properly develop and maintain an accurate inventory of all cloud-based services across the City of Houston's information technology enterprise.

Responsible Party: Chris Mitchell

Estimated Date of Completion: December 2019
Assessment of Response: The Management Response fully addresses issues identified in Finding #2.

Finding # 3 – Enterprise Risk Management – Risk Framework

(Inherent Risk Rating = High)

Background: During Part Two, we selected 6 vendors to conduct detailed testing and test compliance with policies, practices, and internal controls (see Finding #1, Background for more details). We reviewed to see if the risk management process provides a thorough assessment of the risk to the business by implementing the cloud processing model and is aligned to enterprise risk management (ERM) if applicable. The following review steps were conducted:

1. Determine if COH has an ERM model.
2. If an ERM model has been implemented, determine if the cloud computing risk assessment is in alignment with the enterprise ERM.
3. Determine if the services provided by the service provider and the processing model selected will limit the availability or execution of required information security activities, such as:
   - Restrictions on vulnerability assessments and penetration testing
   - Availability of audit logs
   - Access to activity monitoring reports
   - Segregation of duties
4. Determine if the risk management approach includes the following:
   - Identification and valuation of assets and services
   - Identification and analysis of threats and vulnerabilities with their potential impact on assets
   - Analysis of the likelihood of events using a scenario approach
   - Documented management approval of risk acceptance levels and criteria
   - Risk action plans (control, avoid, transfer, accept)
5. Determine if, during the risk assessment, the identified assets include both service-provider- and COH-owned assets and if the information security classifications used in the risk assessments are aligned.
6. Determine if the risk assessment includes the service model and the service provider's capabilities and financial condition.

Findings: COH does not have an ERM model, risk management process, nor risk framework.

Recommendation: Creation of an ERM model and risk management process including risk framework and assessment guidelines (collectively an ERM Process). These processes should include the practices and activities that are required to govern and manage risk effectively, including their identification, analysis and management. In most programs, risk is primarily owned by line management with oversight from independent risk, compliance and/or management oversight functions. Both the COSO ERM framework and the COBIT 5 framework are considered best practices in this area and can be used to help established an ERM program.

Department Management Response: HITS will evaluate the development and implementation of a tailored risk framework specific to the governance and management of cloud-based risks. Overall, HITS is currently aligning to the National Institute of Standards and Technology (NIST) Risk Management Framework.

Responsible Party: Chris Mitchell

Estimated Date of Completion: December 2019

Assessment of Response: The Management Response fully addresses issues identified in Finding #3.

Finding # 4 – Service Transition Planning

(Inherent Risk = High)

Background: During Part Two, we selected 6 vendors to conduct detailed testing and test compliance with policies, practices, and internal controls (see Finding #1, Background for more details). We reviewed to see if procedures, capabilities and alternatives are established, maintained and tested, and a state of readiness has been established to transfer cloud computing operations to an alternate service provider in the event that the selected service provider is unable to meet contractual requirements or ceases operations. The following review steps were conducted:

All cloud solutions

1. Determine that the hardware and software requirements and feasibility for moving from the existing service provider (legacy provider) to another provider (new provider) have been documented for each cloud computing initiative.
2. Determine that an alternate service provider for each legacy service provider has been identified and that the feasibility for transferring processes has been evaluated.
3. Determine if the feasibility analysis includes procedures and time estimates to move large volumes of data, if applicable.
4. Determine if the portability process has been tested.

IaaS (Infrastructure as a Service) cloud solutions

1. Determine if the feasibility analysis of transferring from the IaaS legacy service provider involves any proprietary functions or processes that would preclude or delay the transferring of operations.
2. Determine if the portability analysis includes processes to protect the intellectual property and data from the legacy service provider once the transfer has been completed.

PaaS (Platform as a Service) cloud solutions

1. Determine if the feasibility analysis includes identification of application components and modules that are proprietary and would require special programming during transfer.
2. Determine if the portability analysis includes:
   - Translation functions to a new service provider
   - Interim processing until a new service provider is operational
   - Testing of new processes before promotion to a production environment at the new service provider

SaaS (Software as a Service) cloud solutions

1. Determine if the portability analysis includes:
   - A plan to back up the data in a format that is usable by other applications
   - Routine backup of data
   - Identification of custom tools required to process the data and plans to redevelop
   - Testing of the new service provider's application and due diligence before conversion

Findings: For 5 of the 6 vendors, it was unclear who owns the data (T2 did have ownership defined). None of the selected vendors had an alternate service provider identified nor a feasibility/portability analysis conducted.

Recommendation: Although plans to transfer to a different application are not in the near future a transfer process still needs to be developed, evaluated, and documented. Depending on the risk and impact of the individual application, alternate contracts may need to be in place.

Department Management Response: HITS will develop a departmental service transition process that addresses the transfer of cloud computing operations to an alternate service provider in the event that the selected service provider is unable to meet contractual requirements or ceases operations.

Responsible Party: Reenie Askew

Estimated Date of Completion: December 2019

Assessment of Response: The Management Response fully addresses issues identified in Finding #4.

Finding # 5 – Information Risk Management – Contractual Requirements
(Inherent Risk = High)

Background: During Part Two, we selected 6 vendors to conduct detailed testing and test compliance with policies, practices, and internal controls (see Finding #1, Background for more details). We tested to see if risk management controls were in effect to manage risk-based decisions. The following review steps were conducted:

1. Identify the technology controls and contractual requirements necessary to make fact-based information risk decisions. Consider:
   - Information usage
   - Access controls (Assess controls regarding vendor contract management including:
     - Scope of Services
     - Interface with client hardware and software
     - Consistency between City of Houston's IT Controls and Vendor Terms/Conditions, Cyber-Security Responsibilities, and Incident reporting standards
   - Security controls
   - Location management
   - Privacy controls
2. For SaaS, determine that the COH has identified analytical information required from the service provider to support contractual obligations relating to performance, security and attainment of service level agreements (SLAs).
3. Obtain the analytical data requirements, and determine if the COH routinely monitors and evaluates the attainment of SLAs.
4. For PaaS, determine that the COH has identified the information available and the control practices necessary to manage the application and development processes effectively that address availability, confidentiality, data ownership, concerns around e-discovery, privacy and legal issues.
5. Determine if the COH has established monitoring practices to identify risk issues.
6. For IaaS, determine that the COH has identified and monitors the control and security processes necessary to provide a secure operating environment.
7. Determine if the service provider makes available metrics and controls to assist COHs in implementing their information risk management requirements.

We also reviewed to see if SLAs that support the business requirements are defined, accepted by the service provider and monitored by both parties. The following review steps were conducted:

1. Obtain the SLAs; determine if the SLAs reflect the business requirements.
2. Determine that the SLAs can be monitored using measurable metrics and that the metrics provide appropriate oversight and early warning of unacceptable performance.
3. Determine if the SLA contains clauses that ensure services in case of vendor acquisition or changes in management.

Findings: The HITS executives are not using a consistent process to review the contracts and make risk decisions for each service. Due to a lack of standard risk management approach, the contractual requirements that are in place were developed by the vendors and did not address the risk to the City (e.g. data ownership not defied for 5 of the 6 samples, SLAs not in place for SeeClickFix, SLA penalties not defined, survivability of services in the event of vendor being sold or new management not defined).

- The SeeClickFix contract was severely limited in the controls it contained and Service Level Agreements (SLA) do not exist with the vendor.
- The FAMCare contract was limited in the controls it contained.
- The Kronos contract was limited in the controls it contained

Recommendation: As a best practice based on COBIT 5 framework, document and formalize the list of controls/evaluation points to be used by HITS executives to make risk decisions regarding each service and incorporate those into the product selection & evaluation and contract negotiation phases of cloud governance. Additionally, evaluate the risk of the lack of a SLA with the vendor and establish a SLA, or other compensating control, with the vendor.

Department Management Response: In conjunction with Finding #8, HITS will develop and implement a formalized process to evaluate contractual terms with vendors providing cloud services.

Responsible Party: Somayya Scott

Estimated Date of Completion: December 2019

Assessment of Response: The Management Response fully addresses issues identified in Finding #5.

Finding # 6 – Governance of Cloud Computing Services – Survivability of Service
(Inherent Risk = High)

Background: During Part Two, we selected 6 vendors to conduct detailed testing and test compliance with policies, practices, and internal controls (see Finding #1, Background for more details). We reviewed to see if the service level agreement (SLAs) that support the business requirements are defined, accepted by the service provider and monitored by both parties. The following review steps were conducted:

1. Obtain the SLAs; determine if the SLAs reflect the business requirements.
2. Determine that the SLAs can be monitored using measurable metrics and that the metrics provide appropriate oversight and early warning of unacceptable performance.
3. Determine if the SLA contains clauses that ensure services in case of vendor acquisition or changes in management.

Findings: All the SLA's reviewed did not contain clauses that ensure services in case of vendor acquisition or changes in management.

Recommendation: Include clauses for in the survivability of service in the standard terms and conditions that are negotiated with each contract. The survival clause should specify which contract provisions will remain in effect after the termination or expiration of the agreement. Common obligations covered by survivability of service clauses include: Confidentiality, Access to Data, and/or Support.

Department Management Response: HITS will continue to work with the COH Legal Department to ensure contractual language is included in all cloud service provider contracts highlighting specifics regarding provisions that will remain in effect after the termination or expiration of the agreement.

Responsible Party: Reenie Askew

Estimated Date of Completion: December 2019

Assessment of Response: The Management Response fully addresses issues identified in Finding #6.

Finding # 7 – Governance of Cloud Computing Services - Responsibilities for Governance
(Inherent Risk Rating = Medium)

Background: During Part One, we reviewed to see if service level agreements (SLAs) that support the business requirements are defined, accepted by the service provider and monitored by both parties.

Findings: Responsibilities for governance are not formally documented, but are reviewed by IT Operating Committee (ITOC) which represents all businesses.

Recommendation: Formalize roles and responsibilities for the governance process in a way that can be published and used as an ownership and accountability mechanism. A best practice is to use a RACI chart. A RACI (responsible, accountable, consulted, and informed) chart is a matrix of all the activities and/or decision making authorities undertaken in a process set against all the people or roles in the process. At each intersection of activity and role it is possible to assign somebody responsible, accountable, consulted, or informed for that activity or decision.

Department Management Response: HITS will research and develop a cloud governance computing services RACI chart to outline cloud governance responsibilities.

Responsible Party: Reenie Askew

Estimated Date of Completion: December 2019

Assessment of Response: The Management Response fully addresses issues identified in Finding #7.

Finding # 8 – Third-Party Management - Risk Assessment

(Inherent Risk = Medium)

Background: During Part Two, we selected 6 vendors to conduct detailed testing and test compliance with policies, practices, and internal controls (see Finding #1, Background for more details). We reviewed to see if the service provider has established processes to align its operations with requirements of COH. The following review steps were conducted:

1. Determine if the service provider routinely has independent third-party assessments performed and issued.
2. Determine if the scope of the third-party assessment includes descriptions of the following service provider processes:
    - Risk assessments and reviews of facilities (including backup and co-locations) and services for control weaknesses
    - Incident management
    - Business continuity and disaster recovery
    - Definition of critical service and information security success factors and key performance indicators
    - Frequency of assessments
    - Mitigation procedures to ensure timely completion of identified issues
    - Review of legal, regulatory, industry and contractual requirements for comprehensiveness
    - Cloud service provider's oversight of risk from its own critical vendors
    - Terms of use due diligence to identify roles, responsibilities and accountability of the service provider
    - Legal review for local contract provisions, enforceability and laws pertaining to jurisdictional issues that are the responsibility of their service provider

Findings: HITS received the service organization controls (SOC) report for 2 of the 6 cloud providers as part of the contract negotiation and Microsoft's is available for download on their site, but there is not a documented process to review these reports on an annual basis to evaluate risk to the City. Also, the assessment for FAMCare only covered HIPAA compliance topics which does not address all risks to the City.

Recommendation: Require that a service provider's annual SSAE16 SOC Report be delivered to COH and reviewed by HITS for any changes in control effectiveness reported since the prior year. When the vendor does not have a SOC report, evaluate the use of a right to audit clause to conduct a risk assessment of the vendor. Also, for FAMCare COH should conduct a supplemental review of the other risk areas through a SOC report or expanded compliance report.

Department Management Response: HITS will continue to work with the COH Legal Department to ensure contractual language is included in all cloud service provider contracts requiring the formal submission of SSAE16 SOC reports annually. HITS resource constraints will not allow the performance of formal risk assessments on all service providers that do not provide an annual SSAE16 SOC report.

Responsible Party: Chris Mitchell

Estimated Date of Completion: December 2019

Assessment of Response: The Management Response fully addresses issues identified in Finding #8.

EXHIBIT SECTION

Exhibit #1 – Acknowledgement Statement

DocuSign Envelope ID: CE21836A-1647-441A-8189-21B9F44CD55A

Acknowledgement Statement

Date:

Chris B. Brown
City Controller
Office of the City Controller

**SUBJECT: HOUSTON INFORMATION TECHNOLOGY SERVICES CLOUD APPLICATION GOVERNANCE PERFORMANCE AUDIT REPORT–
ACKNOWLEDGEMENT OF MANAGEMENT RESPONSES**

I acknowledge that the management responses contained in the above referenced report are those of the Houston Information Technology Services (HITS) Department. I also understand that this document will become a part of the final audit report that will be posted on the Controller's website.

Sincerely,

DocuSigned by:
Lisa Kent
5/14/2018
Lisa Kent, Director
Houston Information Technology Services

THIS PAGE INTENTIONALLY LEFT BLANK