

OFFICE OF THE CITY CONTROLLER



**HOUSTON INFORMATION TECHNOLOGY SERVICES
INFORMATION TECHNOLOGY PROCESSES PERFORMANCE
AUDIT**

Chris B. Brown, City Controller

Courtney E. Smith, City Auditor



**OFFICE OF THE CITY CONTROLLER
CITY OF HOUSTON
TEXAS**

CHRIS B. BROWN

June 27, 2018

The Honorable Sylvester Turner, Mayor
City of Houston, Texas

**SUBJECT: REPORT #2018-11
HOUSTON INFORMATION TECHNOLOGY SERVICES – INFORMATION TECHNOLOGY
PROCESSES PERFORMANCE AUDIT**

Mayor Turner:

The Office of the City Controller's Audit Division has completed a performance audit of selected information technology (IT) processes and procedures performed by the Houston Information Technology Services (HITS) Department. HITS provides enterprise IT services including voice and network, cyber-security, email and communication platforms and shared enterprise applications for City of Houston employees. The Department's vision is to be an information and technology organization recognized for collaborative partnership, proactive leadership, strategic innovation, and quality of customer service.

After conducting our initial research based on ordinances, policies, and discussions with key personnel to gain an understanding of the processes under review, we refined our audit objectives to be the consideration of internal controls related to:

- Data backup and recovery;
- Mobile device management; and
- Monitoring vendor contracts.

The initial scope included current processes for vendor contract management and system data backups and recovery. Mobile device data was reviewed for the period February 2017 through July 2017.

We noted that HITS executive leadership has begun implementing strategic department-wide changes and accordingly, the department is presently in a state of transformation with the fundamental goal of providing solutions that serve, protect and enlighten the citizens of the City of Houston.

During our audit, we discovered billings of approximately \$365,000 resulting from mobile device data overage charges that occurred from February 2017 through July 2017.

We also determined a need to strengthen controls related to:

- System data backup and recovery processes;
- Mobile device management; and
- Vendor contract performance monitoring.



**OFFICE OF THE CITY CONTROLLER
CITY OF HOUSTON
TEXAS**

CHRIS B. BROWN

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

TABLE OF CONTENTS

TRANSMITTAL LETTER.....	i
EXECUTIVE SUMMARY.....	1-4
INTRODUCTION.....	1
BACKGROUND.....	1-2
AUDIT SCOPE AND OBJECTIVES.....	2
PROCEDURES PERFORMED.....	2
AUDIT METHODOLOGY.....	3
CONCLUSIONS AND SIGNIFICANT ISSUES.....	3
ACKNOWLEDGEMENT AND SIGNATURES.....	4
DETAILED FINDINGS AND RECOMMENDATIONS.....	5-15
1. NO FORMAL WRITTEN POLICIES AND PROCEDURES.....	5-6
2. SYSTEM BACKUPS ARE NOT STORED OFFSITE.....	7-8
3. SYSTEM BACKUPS ARE NOT TESTED PERIODICALLY.....	9-10
4. MOBILE DEVICE ORDERS AND DEVICE PICKUP DO NOT REQUIRE SIGNATURES AND ARE NOT RECORDED IN TEMS.....	11-12
5. MOBILE DEVICE PLAN CHARGES ARE NOT REVIEWED.....	13-14
6. NO CONTRACT VENDOR PERFORMANCE ASSESSMENT REVIEWS.....	15
EXHIBIT.....	16-17
EXHIBIT 1 – ACKNOWLEDGEMENT STATEMENT.....	17

EXECUTIVE SUMMARY

INTRODUCTION

The Office of the City Controller's Audit Division (AD) has completed a performance audit of selected information technology (IT) processes and procedures performed by Houston Information Technology Services (HITS). The audit considered compliance with City of Houston IT policies and the efficiency and effectiveness of procedures in place to ensure: 1) information system's data was backed-up, mobile devices were managed and 3) vendor contracts were monitored. The audit was included in the Fiscal Year 2017 (FY2017) Audit Plan and was a result of our Enterprise Risk Assessment process.

BACKGROUND

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 is comprised of five separate divisions that provide technical services and support. Those divisions, Project Management Office, Enterprise Applications Services, Enterprise Infrastructure Services, Enterprise Cyber-Security and Radio Communication Services collaborate to provide a professional approach combined with innovative solutions while ensuring that customer service remains at the forefront of its objective. These five divisions provide comprehensive, enterprise-level services throughout the City. HITS approaches all solutions by evaluating the customer's short and long-term goals 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.

HITS executive leadership has begun implementing strategic department-wide changes and accordingly, the department is presently in a state of transformation. The Department's vision is to be an information and technology organization recognized for collaborative partnership, proactive leadership, strategic innovation, and quality of customer service.

HITS has shown success in providing project and operational services that are delivered on-time, within budget and with customer service in mind. HITS is constantly seeking opportunities to decrease costs while improving services for all customers. They are continuously searching for ways to use innovation to provide the best quality of service to our internal departments and to our citizens.

As a result, the performance audit focused on the IT processes geared towards the support, safeguarding, and enhancement of the City's operations. We performed procedures to assess

IT risks to the City's operations, and management's response to the risks identified. While certain exceptions were noted during our audit, the audit team observed that HITS' management has established good controls overall and supervisors and staff were well-trained and professional. The department also has effective controls in place to establish data back-up parameters as well as controls to monitor vendor contract expenditures.

AUDIT SCOPE AND OBJECTIVES

After conducting our initial research based on ordinances, policies, and discussions with key personnel to gain an understanding of the processes under review, we refined our audit objectives to be the consideration of internal controls related to:

1. Data backup and recovery;
2. Mobile device management; and
3. Monitoring vendor contracts.

The initial scope included current processes for vendor contract management and system data backups and recovery. Mobile device data was reviewed for the period February 2017 through July 2017.

PROCEDURES PERFORMED

To obtain sufficient evidence to achieve audit objectives and support our conclusions, we performed the following:

- Communicated with division management, staff, and finance personnel;
- Conducted initial interviews to determine roles, and responsibilities;
- Obtained and reviewed applicable City ordinances administrative policies and vendor contracts;
- Performed site visits of data centers;
- Performed risk assessment and reviewed process control flowcharts;
- Developed audit work program;
- Obtained and reviewed transaction data from Verizon's online customer reporting portal;
- Obtained and reviewed copies of mobile device invoices; and
- Performed substantive testing and documented the results of mobile device vendor billing transactions.

AUDIT METHODOLOGY

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards and in conformance with the International Standards for the Practice of Internal Auditing as promulgated by the Institute of Internal Auditors. 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 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 the overall internal control structure of HITS. 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. Each conclusion is aligned with the related Audit Objective for consistency and reference. 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.

CONCLUSION 1 – (AUDIT OBJECTIVE #1)

Based on audit procedures performed, we noted that HITS has effective controls in place to establish backup parameters for City departments however, there is a need to strengthen controls related to system data backup and recovery offsite storage processes. (See Findings #1, #2, and #3)

CONCLUSION 2 – (AUDIT OBJECTIVE #2)

Based on audit procedures performed, there is a need to strengthen controls over mobile devices management. (See Findings #4, and #5)

CONCLUSION 3 – (AUDIT OBJECTIVE #3)

Based on audit procedures performed, we conclude there are opportunities for strengthening internal controls over vendor contract performance monitoring. (See Finding #6)

Office of the City Controller
Audit Division



ACKNOWLEDGMENT AND SIGNATURES

The Audit Team would like to thank the management and staff of HITS for their cooperation, time, and efforts throughout the course of the engagement. We would also like to thank HITS management for their proactive approach to risk management, and timely remediation of audit findings by correcting issues once identified.

A blue ink signature of David Baszile, written in a cursive style, positioned above a horizontal line.

David Baszile
Assistant City Auditor III

A blue ink signature of Olaniyi Oyedele, written in a cursive style, positioned above a horizontal line.

Olaniyi Oyedele, CPA
Audit Manager

A blue ink signature of Courtney Smith, written in a cursive style, positioned above a horizontal line.

Courtney Smith, CPA, CIA, CFE
City Auditor

DETAILED FINDINGS, RECOMMENDATIONS, MANAGEMENT RESPONSES, AND ASSESSMENT OF RESPONSES

**FINDING #1 – No FORMAL WRITTEN POLICIES AND PROCEDURES
(RISK RATING = HIGH)**

BACKGROUND:

Policies and procedures provide guidance for achieving management’s objectives. Effective policies and procedures define the steps employees should take when performing responsibilities associated with their job functions. They promote operational consistency and uniformity as well as assist in maintaining quality control. Using policies and procedures in employee training helps to foster consistency in practice and reinforces department management’s expectations.

According to Section 2210.A3 of the Institute of Internal Auditors’ (IIA) International Standards for the Professional Practice of Internal Auditing, adequate criteria are needed to evaluate governance, risk management, and controls. Internal auditors must ascertain the extent to which management and/or the board has established adequate criteria to determine whether objectives and goals have been accomplished. The existence of written policies and procedures has been established as one of the criteria for this evaluation.

Additionally, policies and procedures facilitate compliance with City, State, or Federal guidelines, ordinances, laws, and regulations as well as other standards and best practices embodied within industry-specific frameworks critical to HITS’ mission.

During the course of our audit, we performed procedures to determine whether management had written policies and procedures in place to govern its operations.

FINDING:

During the course of our audit we noted that HITS had no formal written approved departmental policies and procedures covering the following operations:

- Vendor contract management;
- System data backup and restores; and
- Mobile device assignment and usage.

RECOMMENDATION:

HITS should create, develop and finalize formally written departmental policies and procedures for all IT processes. Written policies and procedures are considered best practice because they provide uniformity and consistency in operations and can serve as reference tools for existing staff and provide training materials for new employees.

HITS' MANAGEMENT

RESPONSE:

HITS acknowledges that formal policies governing vendor contract management, system and data backup restores and mobile device assignment and usage as nonexistent. These deficient areas were already identified and plans to develop appropriate polices are documented on the HITS Cyber Division's 4-Year Master Plan. The following are details on the alignment of planned policies and specific content that will be addressed:

No.	Policy Title	Addressed Audit Finding
1	System and Services Acquisition	Vendor contract management
2	Business Continuity and Disaster Recovery	System data backup and restores
3	Mobile Device Management	Mobile device assignment and usage

RESPONSIBLE PARTY: TBD

ESTIMATED DATE OF COMPLETION: December, 2019

ASSESSMENT OF

RESPONSE:

Management responses as presented, sufficiently address the issues identified and corrective actions are appropriate.

**FINDING #2 – SYSTEM BACKUPS ARE NOT STORED OFFSITE
(RISK RATING = HIGH)**

BACKGROUND:

The National Institute of Standards and Technology (NIST) Special Publication 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems, section 3.3. Identify Preventive Controls; identifies several steps that an entity can take to reduce the impact of disaster recovery. Such steps include:

- Routinely duplicating or backing up data files, computer programs and critical documents with off-site storage;
- Heat-resistant and waterproof containers for backup media and vital non-electronic records;
- Fire suppression systems;
- Fire and smoke detectors; and
- Appropriately sized uninterruptible power supplies (UPS) to provide short-term backup power to all system components (including environmental and safety controls).

NIST Section 3.4.2, notes that data backup policies should designate the location of stored data, file-naming conventions, media rotation frequency and method for transporting data offsite. It further indicates that storage of back-up data offsite is a good business practice.

On a routine basis as defined by city department, state and local laws or standards, city data, computer programs, and other critical system files are backed up to disk or tape storage by HITS.

We performed procedures to assess the readiness of HITS to restoring the operations of the city in the event of a major disruption in operations.

FINDING:

We observed that HITS does not store system and critical data backups at an offsite storage facility, which could lead to potential and permanent loss of information and disruption in the resumption of operational activities in the event of a major disaster.

RECOMMENDATION:

We recommend that HITS establish an offsite data backup storage sites for all critical data backups in accordance with the NIST requirements.

HITS' MANAGEMENT

RESPONSE:

HITS is not in agreement with the finding. HITS currently backs up data and information to hardened data centers. NIST acknowledges that replication of data from one data center to another meets the requirement. Although replication was not in place at the time of the audit, the deficiency was already identified and an FY18 project had been planned; funding became available July 1, 2018. The backup enhancements were implemented in FY18 and are well documented. Replication of data is scheduled to be completed by the end of 1Q FY19.

RESPONSIBLE PARTY: N/A

ESTIMATED DATE OF COMPLETION: N/A

ASSESSMENT OF

RESPONSE:

During the audit fieldwork review, we were informed that all system backups were performed locally in each data center and were not provided any supporting documentation reflecting planned projects to resolve this issue. We acknowledge that management has since implemented data replication to alternate data centers to mitigate the risk of data loss and that they hope to have the process completely implemented by the 1st quarter of 2019. We appreciate the expeditious manner in which they are addressing risk in this area.

FINDING #3 – SYSTEM BACKUPS ARE PERIODICALLY NOT TESTED

(RISK RATING = HIGH)

BACKGROUND:

Data protection is an essential component of system management. System failure can occur in various instances; hardware can fail, the software has bugs and users make mistakes, hackers can infiltrate the system, unfavorable weather or terrorist activities may damage the system etc. requiring the need for a disaster recovery. Because of this, periodic system backups have become an essential component in IT risk management and governance.

While system backups are considered an essential element of IT risk management, equally important in managing IT risk is the periodic testing of information held within the backup systems. Testing the process of restoring and recovery of back-up data accomplishes two purposes 1) it validates that the process of restoration in the event of a disruption in operations works and 2) it provides a benchmark to ensure that the recovery process can be completed within agreed service level time limits. Decisions related to backup and testing of those backups should be included in the department Continuity of Operations Plan (COOP).

During the course of the audit, we performed procedures to determine whether system backups are periodically tested.

FINDING:

Audit procedures revealed that HITS does not periodically perform routine backup restore process to test the integrity and accuracy of data maintained and ensure that backups are performing as designed.

RECOMMENDATION:

We recommend that HITS formalize data backup testing procedures for all critical data backups and incorporate those procedures into the COOP to ensure:

- the integrity of transactions and data held in storage
- information from the most recent backup process is available
- disruptions in operations can be restored with minimal loss

HITS' MANAGEMENT

RESPONSE:

HITS will develop a procedure to routinely test data backup to restore processes designed to test the integrity of data backups.

RESPONSIBLE PARTY: TBD

ESTIMATED DATE OF COMPLETION: December, 2019

**ASSESSMENT OF
RESPONSE:**

Management responses as presented, sufficiently address the issues identified and corrective actions are appropriate.

FINDING #4 – MOBILE DEVICE ORDERS AND DEVICE PICKUP DO NOT REQUIRE SIGNATURES AND ARE NOT RECORDED IN TEMS

(RISK RATING = HIGH)

BACKGROUND:

The City of Houston Administrative Procedure (AP) No. 8-8 *Mobile Device Eligibility* sub-section 10.1.6 outlines that department wireless coordinators are responsible for placing orders for mobile devices, wireless services and modifications of plans on behalf of users, using the Telecom Expense Management Software (TEMS) system. AP 8-8 indicates that TEMS is to be the City's electronic system designed for the recording of all mobile device related invoices and charges which will then be charged to applicable cost centers.

We performed procedures to determine whether mobile device orders were properly authorized and in accordance with the provisions of Section 10.1.6 requiring the use of TEMS for the placement of orders.

FINDING:

Audit procedures performed revealed that for transactions occurring during our audit scope period (February 2017 through July 2017) TEMS had not been implemented. In addition, HITS does not require any form of management approval verification from wireless coordinators or verification that devices are being requested for eligible users.

RECOMMENDATION:

HITS should ensure that orders for mobile devices have been appropriately approved by management and that the requested devices are for eligible users. In addition, HITS should ensure that the department's procedures are in line with the requirements of AP 8-8 by fully implementing TEMS or by making the appropriate revisions to AP 8-8.

HITS' MANAGEMENT

RESPONSE:

HITS is in the process of fully implementing a Telecom Expense Management System (TEMS) to support and manage the inventory, ordering, and billing of COH wireless devices and voice services. As a stop gap solution, HITS currently utilizes our wireless providers portal to purchase, upgrade and activate new devices, and, to provide usage reports and billing inquiries. The stop gap solution proved to be adequate as HITS was able to produce and provide usage data to the SavingsStat wireless dashboard (<http://citypointe/govt/mayor/HouStat/sstat/>) for review by Department Directors. Lastly, TEMS is not intended to perform as a device approval tool. Departments will be



required to develop internal policies to manage device eligibility, justification and submit evidence of approval.

RESPONSIBLE PARTY: TBD

ESTIMATED DATE OF COMPLETION: December, 2019

**ASSESSMENT OF
RESPONSE:**

Management responses as presented, sufficiently address the issues identified and corrective actions are appropriate.

**FINDING #5 – MOBILE DEVICE PLAN CHARGES ARE NOT REVIEWED
(RISK RATING = HIGH)**

BACKGROUND:

The contract between the City of Houston and Verizon Wireless allows a variety of wireless devices to be provided through available wireless plans. Verizon provides the mobile device as part of the monthly usage charge. The City of Houston is not charged for devices unless the device is lost or stolen. Devices are not tracked, only the phone numbers of the devices and the call/data plan used by the mobile device user. The City of Houston Administrative Procedure No. 8-8 *Mobile Device Eligibility* section 6.2 provides that department wireless coordinator will monitor mobile device spending for devices recorded in TEMS, including reviewing usage and consumption and trend analysis reports at the individual user level.

Furthermore, the provisions of AP 8.8 Section 10.1.2 requires each wireless coordinator review mobile plan usage and determine if the device user's charges are in-line with the user's plan. Many mobile devices are on a limited data or call limit. When users exceed their plan limits the coordinator should verify the need to move the user to a more appropriate plan.

We performed procedures to determine whether there was a process for the monitoring of data usage and consumption to determine whether mobile devices are on appropriate plans. In addition, we obtained and reviewed 6-month of mobile device billing for the period February 2017 through July 2017.

FINDING:

Audit procedures performed revealed that many department wireless coordinators do not review mobile device usage monthly billing charges. Some users on limited data plans are exceeding monthly data allowances resulting in additional charges to the COH.

Because some of these departments mobile device coordinators are not reviewing monthly invoicing, the city is paying unnecessary additional data charges for some mobile device users on limited rather than unlimited data plans. Our review of the six (6) months of mobile device billing (February 2017 – July 2017) showed the City was billed approximately \$365,000.00 in overage charges.

Additionally, a review of three (3) months of data for mobile devices with no device usage (Mobile devices were not used) was over \$6,500 of monthly revenue representing 185 mobile devices which could have resulted from lost phones not reported and services canceled or phones of staff who are no longer with the city not reported to HITS for service cancellation. Inactive mobile devices could represent users being assigned a mobile that has no real need for the device resulting in additional charges to the city.

RECOMMENDATION:

HITS should implement a review system to ensure department coordinators have information regarding users going over assigned data plans which result in additional costs to the City of Houston.

Furthermore, we recommend amendments to the City of Houston's Administrative Procedure No. 8-8 *Mobile Device Eligibility* to allow HITS oversight of department wireless coordinators. A designated HITS person should prepare and review monthly reports to ensure data usage charges are in line with data plans assigned to staff.

HITS' MANAGEMENT

RESPONSE:

Effective January 2018, HITS moved most COH device users to an unlimited plan to eliminate service overage charges. HITS will continue to review usage reports to identify any discrepancies requiring adjustment. In terms of device eligibility, HITS will defer selection and approval to the individual departments responsible for funding devices to approve. Regarding recommended modifications to AP 8-8 and assigning HITS *additional* responsibility to oversee wireless coordinators and provide monthly reports on data usage, HITS will engage the IT Governance Board and IT Operating Committee to identify effective financial and eligibility controls.

RESPONSIBLE PARTY: TBD

ESTIMATED DATE OF COMPLETION: N/A

ASSESSMENT OF

RESPONSE:

Management responses as presented, sufficiently address the issues identified and corrective actions are appropriate.

**FINDING #6 – No CONTRACT VENDOR PERFORMANCE ASSESSMENT REVIEWS
(RISK RATING = MED)**

BACKGROUND:

The City of Houston enters into various contracts with third-party entities (vendors, contractors, consultants etc.) for the provision of goods and/or services in the course of its operations. As part of effort towards managing risks involving contracts and ensuring proper contract administration, management introduced the vendor performance assessment review as a tool towards providing adequate oversight while ensuring that the terms of the contracts are adhered to.

Section 5.1 of AP 5-13 *Performance Evaluation* requires that Departments shall conduct performance evaluations on a regular basis for all vendors, consultants, and contractors holding City contracts. Evaluations should be submitted to the Chief Procurement Officer (CPO) per Section 5.2 of AP 5-13.

FINDING:

HITS has not created nor implemented a periodic vendor performance assessment process to evaluate vendor contract performance for future renewals as well as ensuring compliance with current contract requirements, as required under the provisions of Section 5.1 of AP 5-13.

RECOMMENDATION:

HITS should begin providing vendor contract performance evaluations for all vendor contracts and submit to the CPO in accordance with the requirements of Section 5.2 of AP 5-13.

HITS' MANAGEMENT

RESPONSE:

HITS will utilize the Contractor Performance Evaluation form created by Strategic Purchasing to evaluate vendor contract performance.

RESPONSIBLE PARTY: TBD

ESTIMATED DATE OF COMPLETION: December 2019

ASSESSMENT OF

RESPONSE:

Management responses as presented, sufficiently address the issues identified and corrective actions are appropriate.

EXHIBIT 1

ACKNOWLEDGEMENT STATEMENT

HOUSTON INFORMATION TECHNOLOGY SERVICES DEPARTMENT

Acknowledgement Statement

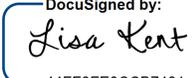
Date:

Chris B. Brown
City Controller
Office of the City Controller

**SUBJECT: HOUSTON INFORMATION TECHNOLOGY SERVICES IT PROCESS 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:

5/14/2018
44FF0FE9CCB7481...

Lisa Kent, Director
Houston Information Technology Services

THIS PAGE INTENTIONALLY LEFT BLANK
