Cybersecurity Audit (Interim Report)

December 18, 2020

City of Fort Worth
Department of Internal Audit

200 Texas Street
Fort Worth, Texas 76102

Audit Staff

Patrice Randle, City Auditor
John Riggs, Assistant City Auditor
Tom Wilson, IT Auditor

Mayor

Betsy Price

Council Members

Carlos Flores, District 2
Brian Byrd, District 3[††]
Cary Moon, District 4[†]
Gyna Bivens, District 5
Jungus Jordan, District 6[††]
Dennis Shingleton, District 7[††]
Kelly Allen Gray, District 8
Ann Zadeh, District 9

[†] Audit Committee Chair
[††] Audit Committee Member

The Cybersecurity Audit is being conducted as part of the Department of Internal Audit's Fiscal Year 2020 Annual Audit Plan.

Audit Objective

The objective of this audit is to evaluate the effectiveness and efficiency of existing controls that would help deter, prevent and/or respond to cyberattacks.

Audit Scope

Our audit included information technology policies, processes and mechanisms in place during FY2020.

Opportunities for Improvement

Up-to-date Continuity of Operations (COOP) plans

Up-to-date ITS security Administrative Regulations

Creation of a vulnerability management plan

Implementation of prior audit recommendations

Summary of Interim Audit Results

As a part of our FY2020 Annual Audit Plan, the Department of Internal Audit is conducting a Cybersecurity Audit. This interim report is to inform management of our progress-to-date, since the audit will be completed over an extended period of time. This report focuses on our review of the City's public internet website, risk assessment processes, information security policies, network monitoring policies and procedures, physical computer assets and software inventories, and management's implementation of prior internal audit findings.

- City of Fort Worth Network Account Password Requirements – We concluded that requirements were adequate and appropriate for ensuring effective control of and access to the City's network.

- Security Awareness Training Program – The program is compliant with the State of Texas' security awareness training reporting requirements.

- Multi-Factor Authentication – The City successfully implemented a new process requiring additional authentication of network account credentials. This process provides enhanced security for users who connect remotely to the City's Virtual Private Network (VPN).

- Continuity of Operations (COOP) Plans – The City has departmental COOP plans. However, a formal process for the management and maintenance of those plans did not exist. COOP plans existed for most, but not all, departments. In some instances, departmental COOP plans had inaccurate information and/or were outdated.

- Information Technology (IT) Security Administrative Regulations – The City has written regulations that address IT security. However, those regulations were not all updated.

- System/Network Vulnerability and IT Change Management – An organizational vulnerability management plan did not exist, and the Information Technology Solutions Department's change management entries did not contain sufficient detail to explain what software was being changed, nor which computer assets were affected by the change(s).

- Implementation Status of Prior Audit Findings – Three recommendations from the IT Asset Accountability internal audit, released in August 2017, had not been implemented.

Additional interim Cybersecurity Audit reports will be issued if we identify significant findings/internal control weaknesses that we feel should be communicated prior to the release of the final report. Each interim report finding will be included in the final report, along with management’s responses.

We would like to thank the Information Technology Solutions Department for their continued help and cooperation thus far.

Table of Contents

Background

Cybersecurity, as defined by the cybersecurity company Norton LifeLock, is the practice of protecting electronic systems, networks, computers, mobile devices, programs and data from malicious digital attacks. Norton LifeLock notes the following as different types of cyber security.

- *Network security* protects internal networks from intruders, by securing infrastructure. Examples of network security include the implementation of two-factor authentication (2FA) and new, strong passwords.

- *Application security* uses software and hardware to defend against external threats that may present themselves in an application's development stage. Examples of application security include antivirus programs, firewalls and encryption.

- *Information security* protects both physical and digital data (essentially data in any form) from unauthorized access, use, change, disclosure, deletion, or other forms of malfeasance.

- *Operational security* addresses processes and decisions for handling and protecting data assets, and includes permissions users have when accessing a network.

- *Data loss prevention* consists of developing policies and processes for handling and preventing the loss of data, and developing recovery policies in the event of a cyber security breach. This includes setting network permissions and policies for data storage.

- *End-user education* involves teaching users to follow best practices, such as refraining from clicking on unknown links or downloading suspicious email attachments, which could allow malware or other forms of malicious software to penetrate the computer network.

Objective

The objective of this audit is to evaluate the effectiveness and efficiency of existing controls that would help deter, prevent and/or respond to cyberattacks.

Scope

The audit included a review of the City's information technology policies, processes and mechanisms in place during FY2020.

Methodology

To achieve the audit objective, the Department of Internal Audit used a detailed audit program based on the cybersecurity framework from the National Institute of Standards and Technology (NIST). We also interviewed staff from the Information Technology (IT) Solutions Department, and reviewed the City's:

- computer assets and software inventory in use by City of Fort Worth (CFW) departments;
- written, information security policies;
- IT Solutions Department's risk assessment processes;
- public internet website;
- lists of security awareness training attendees;
- procedures and listings related to computer asset disposal;
- IT Solutions Department response to physical and electronic anomalous activity events; and,
- network vulnerability scan results.

We conducted this performance audit in accordance with 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We are independent per the generally accepted government auditing standards requirements for internal auditors. Chapter XXVIII of the Fort Worth City Charter established the CFW's Department of Internal Audit independent of management, reporting directly to the Fort Worth City Council. We utilized the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework when evaluating internal controls.

The following internal control components and corresponding principles were considered significant to the audit objective. COSO is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence.

Internal Control Component	Principles
Control Environment	Managerial oversight, integrity, ethics and responsibility; staff recruitment, development, retention, performance and accountability
Control Activities	Policies, procedures and systems
Risk Assessment	Clearly-defined objectives to identify risks, define risk tolerances, and implement necessary controls (e.g., written policies and procedures)
Information and Communication	Communication of necessary quality information
Monitoring	Monitoring and evaluating the effectiveness of internal controls

Audit Results

Based on our test results, the IT Solutions Department has taken measures to help safeguard the City against cyber attacks. We reviewed CFW network account password requirements, and found them to be adequate and appropriate for ensuring that access to CFW network and related software systems is effectively controlled. We also reviewed the IT Solutions Department's security awareness training program, and determined that it was in compliance with the state of Texas' security awareness training reporting requirements. In October 2020, the IT Solutions Department implemented a multi-factor authentication process that provides enhanced security for users who connect remotely to the City's Virtual Private Network (VPN).

Six departmental Continuity of Operations (COOP) plans contained incorrect contact (primary and alternate) information, and 10 department plans contained no information regarding dates of last review/update.

The IT Security Policy, referred to as AR-D5, contains detailed information regarding the CFW's information security program, including roles and responsibilities, and physical and logical security controls. AR-D5 was scheduled for review by June 30, 2015. However, we could not determine if the review occurred. We did note that AR-D5 did not mention current state of Texas security awareness training reporting standards or the multi-factor network account access process. The multi-factor network account access process was only recently completed (in October 2020).

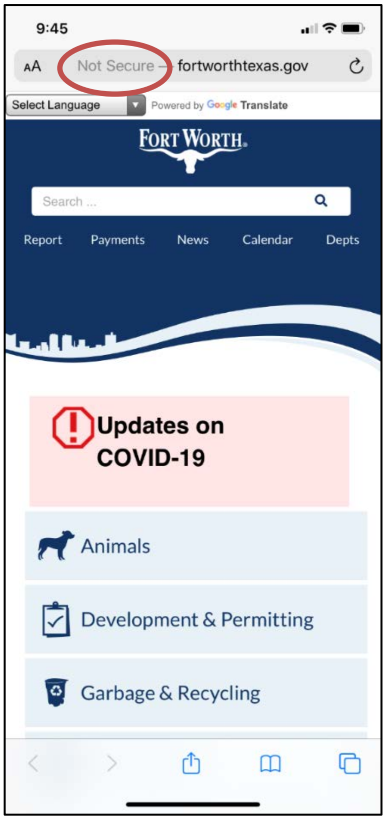
We were unable to locate documentation supporting a correlation between identified system/network vulnerabilities, and system/network software patch installations and updates. Lack of documentation makes verification of effectiveness difficult. Additionally, the City's IT change management processes did not provide sufficient details regarding what software was being implemented and/or changed, nor was information provided as to which CFW computer assets/programs were affected.

Previous issues identified in the IT Asset Accountability Audit (released by the Department of Internal Audit in FY2017) had not been implemented as of September 2020. The three Internal Audit recommendations addressed the lack of full accountability of IT assets purchased by the CFW, and the lack of written City-wide policies and procedures to govern the CFW's IT inventory. Accurate and efficient IT asset accountability is a basic and necessary component of a successful cybersecurity program. The inability to accurately account for purchased and deployed IT assets poses risks to the organization, such as theft of assets, as well as potential delays in applying required software and anti-virus updates.

The City conducts self-assessments to determine compliance with procurement card industry standards. In March 2019, the IT Solutions Department completed an assessment of compliance with Payment Card Industry Data Security Standard (PCI-DSS) requirements. Based on self-assessment results, the IT Solutions Department identified areas within the Park and Recreation, Development Services and Fire Departments that did not have PCI-compliant credit card machines. The non-compliance issues were self-reported to J. P. Morgan Chase, and the CFW was fined a total of $55,000.00 for the period May 2019 through March 2020. The IT Solutions Department subsequently updated their policies and procedures to ensure compliance with PCI-DSS standards, and assisted with the replacement of the non-compliant credit card machines. In July 2020, Weaver & Tidwell, LLC performed a specific attestation engagement and issued the City an Attestation of Compliance.

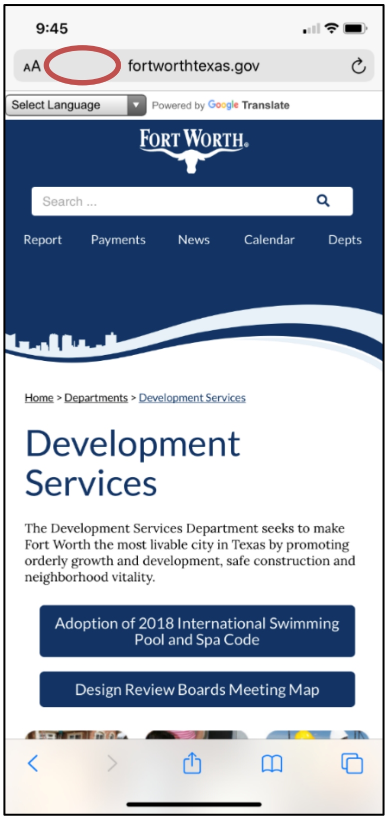
As shown in the following images, we noted that the City's public website was not fully secured, using encrypted connections (https) during our audit testing. However, the recent website conversion on October 19, 2020 remediated the security issue by providing an encrypted connection for all pages.

Image 1: CFW Main Web Page



Updates on COVID-19

Image 2: CFW Development Services Web Page


9:45
AA
fortworthtexas.gov
Select Language
Powered by Google Translate
FORT WORTH
Search ...
Report
Payments
News
Calendar
Depts
Home > Departments > Development Services
Adoption of 2018 International Swimming Pool and Spa Code
Design Review Boards Meeting Map

Development Services

The Development Services Department seeks to make Fort Worth the most livable city in Texas by promoting orderly growth and development, safe construction and neighborhood vitality.

Source: Public Internet

Detailed Audit Findings

1. Continuity of Operations (COOP) Plans did not exist for each City department, and some existing COOP Plans were not up-to-date.

We reviewed the current CFW Continuity of Operations plans for each department, and noted the following:

Department	Existing Plan	Departmental Contact Information	Date Last Updated Known / Unknown
Aviation	Yes	Incorrect/Missing	Known
City Secretary's Office	Yes	Incorrect/Missing	Unknown
Code Compliance	Yes	Correct	Unknown
Communications & Public Engagement	Yes	Correct	Known
Development Services	Yes	Correct	Known
Diversity & Inclusion	Yes	Correct	Known
Economic Development	Yes	Correct	Known
Financial Management Services	Yes	Correct	Unknown
Fire	Yes	Incorrect/Missing	Unknown
Human Resources	Yes	Correct	Known
Internal Audit	Yes	Incorrect/Missing	Unknown
IT Solutions	Yes	Incorrect/Missing	Known
Law	Yes	Correct	Unknown
Library	Yes	Correct	Unknown
Municipal Court	Yes	Correct	Known
Neighborhood Services	Yes	Incorrect/Missing	Known
Office of Emergency Management	Yes	Correct	Known
Park & Recreation	Yes	Correct	Unknown
Performance & Budget	Yes	Correct	Unknown
Planning & Data Analytics	No	N/A	N/A
Police	Yes	Correct	Known
Property Management	Yes	Correct	Unknown
Public Events	Yes	Correct	Known
Transportation & Public Works	Yes	Correct	Known
Water	Yes	Correct	Known

With the exception of the Fire Department, City departments that are responsible for more critical operations (e.g., Communications and Public Engagement, Police, Transportation and Public Works and Water Departments) had updated COOP plans. As noted in the preceding table, the Fire Department had a COOP plan; however, that plan was not up-to-date.

A COOP plan was on file for the Performance and Budget Department, but not on file for the Planning and Data Analytics Department. As a result of a January 2020 reorganization, functions and responsibilities previously assigned to the Performance and Budget Department were reassigned to other departments, including the Planning and Data Analytics Department. The impact of this reorganization had not been fully incorporated into the COOP plans.

Six departments had incorrect/missing information for primary and alternate department contacts, and COOP plans for 10 departments contained no information as to when the plans were last updated. Our review of the COOP plans did not include the verification of department-specific information such as software in use and equipment required for continuity of operations.

According to correspondence within the City's Office of Emergency Management (OEM), departments are requested to submit at least one COOP plan revision/update each year. Additionally, OEM began quarterly department meetings in FY2020. Departments are encouraged to make updates to their plans after each of these meetings, or at any time the department believes an update is necessary. The presence of incorrect and/or outdated information within the COOP plans increases the risk that critical services and systems may not be fully restored or accounted for during the execution of those plans. The 2020 COVID-19 pandemic, resulting in the need for CFW employees to work remotely, is illustrative of the need for CFW departments to possess complete and accurate COOP plans, and for those plans to be reviewed and updated on an established schedule.

The Control Objectives for Information Technologies (COBIT) 2019 standard states that business continuity plans should undergo management review at regular intervals to ensure their continued suitability, adequacy and effectiveness. Additionally, the impact of additions and/or major changes to enterprise organizations, business processes, outsourcing arrangements, technologies, infrastructure and operating/application systems should be reviewed for consideration.

Recommendation 1A: *The Fire Chief, through the Office of Emergency Management's Emergency Operations Manager, should ensure that all CFW departments provide current and up-to-date COOP plan documents for their respective operations.*

Auditee's Response: Concur. The Fire Chief in association with the Emergency Operations Coordinator has confirmed that COOP plans have been submitted by all CFW departments. Those plans can be accessed on the City of Fort Worth's JEOC Sharepoint site at: https://fortworthtexas.sharepoint.com/sites/JEOC/SitePages/Continuity-of-Operations-(COOP).aspx.

Responsibility: Fire – Office of Emergency Management (OEM)

Target Implementation Date: Completed

Applicable Department Head: James Davis, Fire Chief

Applicable Assistant City Manager: Valerie Washington

Recommendation 1B: *The Fire Chief, in cooperation with the Emergency Operations Manager, should ensure that a formal schedule is established and implemented for the update and management of COOP plan documents for all CFW departments.*

Auditee's Response: Concur. The Fire Chief in association with the Emergency Operations Coordinator has developed a plan for having COOP plans updated biennially (i.e., every other year).

Responsibility: Fire – Office of Emergency Management (OEM)

Target Implementation Date: June 30, 2021

Applicable Department Head: James Davis, Fire Chief

Applicable Assistant City Manager: Valerie Washington

2. CFW Administrative Regulations governing IT security were out-of-date.

The CFW's IT Security program is detailed within Administrative Regulation AR-D5. Appendices 1 through 6 of AR-D5 are policy statements that address password administration, data encryption, mobile computing and removable storage, wireless security, extranet and remote network access, and the Payment Card Industry Data Security Standard (PCI-DSS). These appendices provide details as to their purpose, the departments affected and other details specific to the areas addressed. The current version of AR-D5 became effective as of June 12, 2012, and replaced the previous version dated February 8, 2010. AR-D5 and its appendices are published on the CFW's employee intranet.

Based on our test results, AR-D5 has not been reviewed nor updated since June 2012. Additionally, the related appendices contain no information detailing when each one became effective, nor do they show when they were last reviewed or updated. There is also limited information regarding security awareness training, and no references to the new multi-factor network account access process. It should be noted that the new authentication deployment process (which began in March 2020) was only recently completed (in October 2020)**.** Appendix 6 of AR-D5, the City's Payment Card Industry Data Security Standard (PCI-DSS) Policy, was updated during the audit period. However, that policy had not been published to the CFW's intranet.

The Control Objectives for Information Technologies (COBIT) 2019 standard states that an organization's data management strategies, roles, and responsibilities should be defined and communicated, consistent with data management policies and regulations. That standard also references stakeholder approval, reviews and updates, as necessary.

Today's IT environments are in a consistent state of change, and the policies and regulations governing IT environments must remain up-to-date, with any changes published in a timely manner. Infrequent review of IT security documents increases the likelihood that the City's official security policies will become outdated and ineffective, thereby increasing the risk of adverse exposure of the City's network to inside and outside threats.

Recommendation 2A: *The Chief Technology Officer should ensure that all IT security-related Administrative Regulations are reviewed, updated as necessary, and that detailed information regarding the dates of last review and update are present.*

Auditee's Response: Concur. ITS will review security related ARs. Posted documents will be updated with necessary revisions and review dates. Reviews will be performed annually.

Responsibility: ITS Security Team

Target Implementation Date: January 8, 2021

Applicable Department Head: Kevin Gunn, Chief Technology Officer

Applicable Assistant City Manager: Valerie Washington

Recommendation 2B: *The Chief Technology Officer should ensure that a formal schedule for the review and update of IT security-related Administrative Regulations is implemented.*

Auditee's Response: Concur. ITS established a formal schedule for review. ITS will review Security related ARs on an annual basis and document such review.

Responsibility: ITS Security Team

Target Implementation Date: December 30, 2020

Applicable Department Head: Kevin Gunn, Chief Technology Officer

Applicable Assistant City Manager: Valerie Washington

3. Documented processes for system/network vulnerabilities and IT change management activities were inadequate.

The IT Solutions Department performs network vulnerability scans to identify potential threats to the CFW's network. The current vulnerability scan schedule is listed in the following chart.

Vulnerability Scan Type	Frequency	Day(s) of the Week
External-facing systems/network	Weekly	Wednesday, Friday
Internal-facing systems/network	Monthly	1st Thursday of the Month
Perimeter Network (DMZ)	Monthly	1st Tuesday of the Month

Source: CFW IT Solutions Department

- External-facing systems are those used for interaction with/by the public (e.g., Development Services Department and the Fort Worth Municipal Court).
- Internal-facing systems are those used by City employees in the performance of their daily responsibilities (e.g., Hyperion budgeting software and PeopleSoft Financials).
- The perimeter network, also known as the Demilitarized Zone (DMZ), is a network that resides between the external and internal systems. The DMZ is designed to prevent outside connections to external systems from reaching the internal systems.

Although a formal vulnerability scanning schedule exists, we concluded that a formal organizational vulnerability management plan does not. A vulnerability management plan encompasses methodologies and tools used by an organization/entity to identify, classify, remediate, and mitigate vulnerabilities to its IT network. We reviewed documentation provided by the IT Solutions Department, and found inadequacies with the CFW's ability to effectively account for and mitigate identified system and network vulnerabilities. In addition, we reviewed all software-related IT change management system requests processed between July 2019 and June 2020, and were unable to link those changes to identified vulnerabilities.

We also noted that IT change management system entries did not contain sufficient information describing the details of the requests, nor did they provide adequate details as to the impact of the changes made. We reviewed two change requests for Microsoft software updates that were processed in March and April 2020. Neither request provided specific information regarding the software (e.g., name, version, patch level, etc.) that was being updated. Additionally, a Microsoft Windows version upgrade, processed in December 2019, did not list the specific CFW computer assets that were being affected by the change. The lack of details in these change requests raises concerns as to the adequacy of the effectiveness and efficiency of the IT change management process.

The Control Objectives for Information Technologies (COBIT) 2019 standard states that the network infrastructure should be monitored for security-related events; vulnerabilities and threats should be managed; and such monitoring and management activities should include the use of various tools and technologies to identify vulnerabilities and threats, along with processes to appropriately disseminate and report on the identified items. The COBIT standard also states that preventative, detective, and corrective measures should be implemented and maintained (especially up-to-date security patches and virus control) across the enterprise to protect information systems and technology from malicious software.

Recommendation 3A: *The Chief Technology Officer should ensure that formal threat intelligence dissemination and reporting processes are developed. Such processes should readily enable the organization to manage threats which could adversely impact the organization's ability to provide IT-related services and support to the City of Fort Worth.*

Auditee's Response: Concur. ITS Security Team will document the process to manage threat intelligence information. The documents will include actions taken to mitigate those threats.

Responsibility: ITS Security Team

Target Implementation Date: March 30, 2021

Applicable Department Head: Kevin Gunn, Chief Technology Officer

Applicable Assistant City Manager: Valerie Washington

Recommendation 3B: *The Chief Technology Officer should ensure that supporting documentation for software-related IT change requests contain detailed information regarding any software patches and/or updates being applied as part of the request, including the physical computer assets affected.*

Auditee's Response: Concur. ITS Teams will ensure that complete documentation and information exists for security related IT change requests. Patch information may be included in the change record or referenced separately. When appropriate, the specific assets or types of assets will be listed in the change request.

Responsibility: ITS all divisions and teams

Target Implementation Date: March 30, 2021

Applicable Department Head: Kevin Gunn, Chief Technology Officer

Applicable Assistant City Manager: Valerie Washington

4. Prior internal audit recommendations were not implemented.

Internal Audit released an IT Asset Verification Audit on August 4, 2017 that identified two significant findings directly related to IT asset accountability. The objective of this prior audit was to confirm the physical existence and proper disposition of IT assets purchased by and belonging to the CFW. Details regarding those two audit findings and the corresponding audit recommendations that were not implemented are shown in the following table.

Prior Audit Finding	Prior Audit Recommendation	Target Implementation Date	Revised Target Date
1. There is no full accountability of IT assets purchased by the CFW	1A: The Chief Technology Officer should require that ITS identify anomalies that are identified during routine Discovery Tool software runs. Any anomalies, not resolved by ITS, should be communicated to user departments for discrepancy resolution.	Jan 2018	Sept 2022
	1C: The City Manager should require that departments maintain departmental IT inventory listings which should include, at a minimum, asset descriptions, City asset tag numbers, asset serial numbers, assigned user, locations, and should be used to help resolve discrepancies identified during Discovery Tool run (i.e., a computer once detected by the Discovery Tool software is not decommissioned, but has not been detected by Discovery Tool in several weeks or months).	Jan 2018	Sept 2022
2. No written City-wide policies and procedures exist to govern the CFW's IT inventory	2: The Chief Technology Officer should ensure that policies and procedures related to the City's IT inventory are documented within the departmental and city-wide policies and procedures. Any changes in policy and procedures that occur between periodic reviews should be promptly updated as those changes occur.	Jan 2018	Dec 2020

Proper accountability of IT assets is a necessary component of an effective cybersecurity management program. The inability to accurately account for purchased and deployed IT assets poses risks to the organization, such as the theft of assets, as well as potential delays in applying required software and anti-virus updates to those assets.

The IT Solutions Department concurred with our prior audit recommendation which addressed accountability of IT assets purchased by the CFW (Recommendation 1A). The IT Solutions Department stated that the implementation was dependent upon the purchase and implementation of new Discovery Tool software. That effort was initially scheduled to begin in January 2018, and was to be completed by October 2018. However, the new Discovery Tool software was not purchased until March 2020. The IT Solutions Department's target implementation date is now September 2022.

The IT Solutions Department partially concurred with Recommendation 1C, which recommended that departments be required to maintain departmental IT inventory listings. The IT Solutions Department responded that management recognized that the responsibility for managing computer assets was divided between user departments and the IT Solutions Department. User departments funded computer purchases through their operating budget and managed the physical computer asset, while the IT Solutions Department managed software components through the Discovery Tool. The IT Solutions Department stated that beginning in FY2017, funding for the procurement of computer assets was consolidated in the Computer Equipment Replacement Fund, which is managed by the IT Solutions Department. The IT Solutions Department further stated that going forward, they would coordinate with departments to manage the funding, physical assets (including the asset identifying information) and computer asset software components. The recommendation's original target implementation date was January 2018, and is now projected to be September 2022.

The ITS Department concurred with Recommendation 2, and stated they would work with the Purchasing Division to ensure departmental procurement and operating procedures were updated as the new inventory system is implemented. The recommendation's original target implementation date was January 2018. The recommendation is now projected to be implemented this month (December 2020).

The Control Objectives for Information Technologies (COBIT) 2019 standard states that all IT assets should be identified, with associated records created and kept up-to-date. In addition, the existence of all owned assets should be verified by performing regular physical and logical inventory checks and reconciliations. Such activity should include the use of software discovery tools.

Recommendation 4: *The City Manager, in cooperation with the Chief Technology Officer, should ensure that the recommendations from Internal Audit's 2017 IT Asset Verification Audit are implemented by the current dates provided by the IT Solutions Department, if not sooner.*

Auditee's Response: Concur. ITS acknowledges that there have been delays in completing remediation's from the 2017 Asset Verification audit. Personnel performance, staffing levels, department organizational changes, and emergency response activities, have contributed to these delays.

The asset management software system will be completed by 12/30/2020. The asset management administrative directive will be approved by March 31, 2021.

Responsibility: ITS Infrastructure Team

Target Implementation Date: March 31, 2021

Applicable Department Head: Kevin Gunn, Chief Technology Officer

Applicable Assistant City Manager: Valerie Washington

Next Steps

The Department of Internal Audit will continue to provide additional interim reports, if deemed necessary. As our audit testing continues, any additional findings will be articulated within the final audit report, along with our audit recommendations and management's responses.