CITY OF SAN JOSE
CAPITAL OF SILICON VALLEY

Memorandum

TO: SMART CITIES AND SERVICE IMPROVEMENTS COMMITTEE

FROM: Rob Lloyd

SUBJECT: **INFORMATION SYSTEMS AUDIT UPDATES**

DATE: August 9, 2017

Approved [signature] Date 9 August 2017

INFORMATION

On May 4, 2017 the Smart Cities and Service Improvements Committee requested a detailed view on the update of IT audit comments. This report provides the status of all audit recommendations related to the information systems in the City.

BACKGROUND

Since 2012, a number of reviews, comments and findings have accumulated that the Information Technology Department is now working to resolve. A complete list of the recommendations for each of the audit reports and the status of each recommendation can be found in Attachment A and B. The City Auditor's Office (CAO) follows up on the status of open audit recommendations every six months and makes an official report to Council. The next report is scheduled for September 2017 release. This report is a supplement to that work. Similarly, the City's external auditor of Financial Statements, Grant Thornton, is in the process of conducting their audit update and reviewing internal controls on the information systems related to the external Financial Statements audit.

ANALYSIS

Audit of Information Technology General Controls (Issued January 2012)

Total Audit Recommendations	Completed Recommendations	In Progress Recommendations	Queued Recommendations
11	2	6	3

In-Progress: Recommendation #1, 2, 4, 6, 7, 10

Recommendation #1, 2, 4, 6, and 10 – The Information Technology Department (ITD) has made progress (a) to ensure changes to the City's network and mission-critical enterprise systems are coordinated and controlled through change management processes and (b) to improve password and access controls over the City's network and data. A draft information security policy was completed which addresses, among other things, account access, password protocols, technology usage such as ITD responsibilities in enforcement, applying a least-privilege model, acceptable use of computer equipment, and decommissioning computer equipment. ITD is revising a draft policy based on the National Institute of Standards and Technology Cybersecurity Framework, which is expected to be reviewed by the City Council this Fall.

Recommendation #4 – ITD is working with the Finance Department to assist five departments currently processing credit card payments to resolve documentation, training and security requirements necessary to comply with Payment Card Industry – Data Security Standard (PCI-DSS). The documentation is held in a secure, centralized location and workgroups are nearly complete with all necessary documentation and security requirements. Ongoing compliance will be coordinated by the new City Information Security Officer, approved in the 2017-2018 budget process and budgeted to be hired in the Fall.

Recommendation #7 – Initial progress has been made by staff on increasing systems resilience so that computerized operations and data can be recovered in case of unexpected interruptions. ITD ensures the City's critical data is protected by making replicas and backups following business resumption practices. ITD is modernizing its Enterprise Business Resumption Program and related tools and processes. Staff has a goal to complete the project by December 2017.

Queued: Recommendation #5, 8, 9

Recommendation #5 – Staff was asked to publicly post the Identity Theft Prevention Program and add boilerplate language in its contracts to protect the City from liability when Personally Identifiable Information is collected. Draft language has been submitted to the City Attorney's Office and Purchasing Division for review. This recommendation is expected to be completed by December 2018.

Recommendation #8 – ITD is working on a remediation plan to address gaps in the disaster recovery and business resumption plans for critical city-wide systems. In addition, funding was approved to implement a Secondary Data Center at a City facility and is scheduled to be operational with limited backup equipment by December 2017. Once available, more work will be required to implement new processes, including coordinating with stakeholder departments. As part of the City's server infrastructure refresh, staff will analyze the existing environment to determine which applications and servers are most at need due to risk and will migrate them to the new on-premises environment, or cloud services, as appropriate.

ITD will work with departments to migrate all critical City documents to OneDrive and SharePoint by December 2018, both offering built-in data redundancy as part of the cloud services.

Recommendation #9 – ITD is researching and testing different enterprise asset management tools and plans to bring forward a budget request for an IT Asset Management System in the upcoming budget process, should the initiative rank as high priority in the City's technology portfolio and workplan. This tool would provide transparency on IT assets and identify life cycle refresh.

External Audit of Financial Statement (Issued November 2016)

Total Audit Recommendations	Completed Recommendations	In Progress Recommendations	Queued Recommendations
3	0	3	0

In-Progress: Recommendations # 2016-003, 2016-004, 2016-005

City-wide Information Security Program – Although some progress has been made to strengthen internal controls to create a secure and effective information and communication technologies environment, considerable work remains. The effort will be supported by resources added in the 2017-2018 budget to create the City's Information Security Office (ISO). The ISO will serve as the City's enterprise cybersecurity program with assigned responsibilities, the dedication of a City Information Security Officer position, staffing, and funding for training, assessments, and monitoring services. A draft information security policy has been developed and is expected to be reviewed by the City Council this Fall. The external auditor's recommendations will be addressed in the new security policy.

Account Management, Password Configuration, Broad Privileged Access, Password Configuration, Shared Accounts, and Audit Logging/Monitoring – System authorization, access, and account management controls are being implemented to limit system activities on a least-permissive basis. Staff continues to identify options for improved segregation of duties despite limited staffing. Audit findings related to each of these areas for specific information systems remain in progress and will be assigned to the CISO, once hired.

Change Management – Processes and procedures are in progress that will provide assurance that the software, data, and other changes are approved and tested so that the information system operate as intended and are not threatened by security risks. ITD will continue to improve processes and communications with the IT Leadership Group over time. Focus is currently on training and practice with the new protocols.

Customer Call Handling (Issued August 2014)

Total Audit Recommendations	Completed Recommendations	In Progress Recommendations	Queued Recommendations
13	6	7	0

In-Progress: Recommendation #2, 4, 7, 8, 11, 12, 13

Progress has been made to improve the efficiency and effectiveness of customer call handling at the City's Customer Contact Center, as well as in eight smaller customer call teams within various City departments. The City selected a Customer Relationship Management/Service Request Management solution (CRM/SRM) as part of the Amazing Customer Experience/My San Jose project completed July 31, 2017. The 3-1-1 software increases access to the most requested City services (e.g., graffiti abatement, abandoned vehicles, streetlight outages, and potholes) via a mobile application, an on-line portal, online chat, a Frequently Asked Questions knowledgebase for public and staff use, and improves performance management for a superior customer experience. The system pairs with a new call management solution in use since late-2016. Additional training and process improvements will continue. Broader resident and business use is expected and a marketing push for CRM that was coordinated with the City's National Night Out activities on August 1.

The city-wide Customer Service Policy was approved by the City Manager in June and will be deployed in August. Guidelines to improve the customer experience and manage performance are addressed in the new policy.

Technology Deployments: Additional Resources Timelines (Issued March 2016)

Total Audit Recommendations	Completed Recommendations	In Progress Recommendations	Queued Recommendations
9	6	3	0

In-Progress: Recommendation #1, 5, 9

A multi-pronged approach is in place to ensure technology deployments are successful and completed in a timely manner. Some progress has been made identifying the City's key technology systems, the end of life/support for these systems, and the estimated cost to replace them. This technology debt has been incorporated into the 2017 Status Report on Deferred Maintenance and Infrastructure Backlog. However, establishing a continuous replacement program and identifying funding for the program remains difficult for the City due to limited resources across the organization.

The Administration is reviewing the technology procurement protocols and pursuing co-work models wherein ITD staff plays an integral role in technology planning, implementation,

configuration and support of hardware and software solutions with vendors throughout projects, permitting better operational transition when vendor staffs leave. Early results from this new practice over the past eight months have been promising with three major enterprise projects that were successfully delivered.

Mobile Devices: Improvements Needed to Ensure Efficient, Secure, And Strategic Deployment (Issued 12/16)

Total Audit Recommendations	Completed Recommendations	In Progress Recommendations	Queued Recommendations	Declined Recommendation
16	0	10	5	1

In-Progress: Recommendations – #3, 4, 5, 6, 7, 8, 9, 11, 13, 16

Limited progress has been made to increase the management and optimization of mobile devices use. Staff drafted a simpler Mobile Device Policy to reflect current uses and clarify specific duties. Guidelines to ensure that departments regularly verify employee eligibility and clarification on the taxability of stipends are being coordinated with Finance and IT departments. Information security awareness training and a curriculum outlining the specific responsibilities of the departmental mobile device liaisons still need to be developed and rolled out between the Office of Employee Relations and ITD, once the policy is approved and the City Information Security Officer is hired. Streamlining the process to order mobile devices and accessories, regularly updating the City price list for mobile devices, and creating an interdepartmental working groups to serve as a mobile device forum are expected to be implemented by 2018.

Queued: Recommendation #1, 2, 12, 14, 15

Purchasing an inventory management solution; adjusting the amount and structure of the City's cellphone and data stipends; automating ordering of mobile devices; implementing mobile device management software; and training/use of professional telecommunications expense management software should address the City Auditor's recommendations. Staff completed basic analysis on all of the improvements by August 2017. However, the improvements require the addition or reallocation of resources that are not available. The benefits and potential costs to implement these recommendations will be evaluated as part of the annual budget process in light of the City's budget outlook and other city-wide and departmental funding priorities.

Declined: Recommendation #10

The Administration disagrees with the recommendation to consider allowing personal use of City-owned cellular phones for short, infrequent personal calls. With very limited exceptions, City-owned equipment is to be used solely for official City business pursuant to several City Administrative Policy Manual sections and ethics rules.

NEXT STEPS/CONCLUSIONS

As described above, the City continues to make significant progress towards resolution of important recommendations made by the City Auditor and Grant Thornton. Activity made by ITD in the last 10 months on long-dormant audit recommendations will ensure the City's environment of information and communication technologies is effective, secure, and improves the customer experiences of the City's residents and businesses. These goals connect directly to the Innovation and Technology Strategic Plan completed by the Information Technology Department and approved by City Council in March 2017.

Staff will update the Committee in November about additional progress made in addressing information systems audit findings. In addition, ITD will continue to work with the City Auditor's Office to provide the status of open audit recommendations every six months, with the next report expected to be released in September.

/s/
ROB LLOYD
Chief Information Officer

Attachment A: City Auditor's Audit Recommendations
Attachment B: Grant Thornton Financial Statement Information Technology Findings

For questions please contact Rob Lloyd, Chief Information Officer at (408) 535-3566.

 # 12-02 Audit of Information Technology General Control (Issued 1/18/12)
Recommendation #1: To ensure changes to the City's network and mission-critical enterprise systems are tightly controlled, ITD should immediately change the password to its shared administrative account, ensure that administrative log-ins to the City's network are traceable, and strictly limit administrative log-in privileges to those who absolutely need such privileges. Furthermore, we recommend that the ITD CIO annually review and approve the memberships of shared accounts that can access the City's network and enterprise systems, and if necessary make changes based on current business needs.

Status: In Progress

Recommendation #2: To improve password and access controls over the City's network and data, ITD should:
a) Establish minimum length and complexity requirements for users' passwords, automatic periodic expiration schedules, and "lock-outs" when users reach a pre-determined number of consecutive unsuccessful login attempts.
b) While granting access to additional server drives, etc., ITD should by default, terminate transferring employees' access to the drives of the departments they are departing, or explore a system through which employees' access levels are tied to their employment status as recorded in the City's personnel system.
c) Develop a review process requiring departments to periodically review the users with access to their departmental drives.

Status: In Progress

Recommendation #3: The City should include boilerplate terms to include in contracts with third parties the following:
A) Require PCl-DSS compliance when contractors are responsible for collecting credit card information.
B) Require the vendors to submit current PCl-DSS compliance certificates on an ongoing basis.

Status: Completed

Recommendation #4: In order to fully comply with Data Security Standards (PCI-DSS), immediately develop an Information Security Policy and include within this policy (applicable to all users who are connected to the City's network) the following minimum standards:
a) Updated password and access protocols (see Recommendation #2);
b) Required schedules for periodic reviews of people with access to data center (including restricting the number of people with access);
c) Improved guidelines to departments for facilitating IT network changes during inter-departmental transfers and terminations;
d) Training and implementation of the City's information security policy;
e) After developing and implementing a Council-adopted Information Security Policy, initiate a citywide data security assessment to identify City's PCI-DSS status.
Status: In Progress

Recommendation #5: The City should expand its Identity Theft Prevention Program to include all programs that collect personally identifiable information and:
a) Annually review, amend and report on the status of handling private information.
b) Annually review the business needs of employees with access to private information and update accordingly.
c) Provide periodic training for all employees handling private information and/or annually highlight (through an email) and inform employees of their responsibilities on safeguarding this data.
d) Include boilerplate language in its contracts to protect the City from liability when personally identifiable information is collected and ensure that the contractor has controls in place to secure and protect this information.
e) Ensure that the ITPP guidelines are posted publicly and easily accessible by City employees.

Status: Queued

Recommendation #6: We recommend that ITD develop the following written policies and procedures:
a) Internal policies and procedures on day-to-day operations within ITD;
b) Citywide policies on technology usage such as ITD responsibilities in enforcement, principles of least privilege, and acceptable use of computer equipment. Within these policies develop clear guidelines on which departments would be exempt and why, from some of these policies.

Status: In Progress

Recommendation #7: In order to ensure that the City's critical data is protected ITD should:
a) Ensure that backups are done and tapes are sent off-site at the pre-determined intervals;
b) Get end-user input to determine if the current back-up process meets individual departments' business needs and City Council-approved document retention schedules; and
c) Formalize, document and implement these processes.

Status: In Progress

Recommendation #8: ITD take the lead to develop (and test) a Disaster Data Recovery Plan and ensure that end-user business needs are included in the final plan.

Status: Queued

Recommendation #9: ITD should collect, maintain and periodically update a central inventory of computer equipment and software, and should use its inventory management system and records of technology purchases to:
a) better evaluate purchasing needs,
b) identify opportunities to redistribute and/or share equipment and software, and
c) to the extent possible, ITD should pursue opportunities to centrally-install packages, rather than installing packages at individual workstations.

Status: Queued

Recommendation #10: Because computer equipment may contain personal identifiable information and other sensitive information, ITD should develop, distribute, and implement a Citywide policy for decommissioning computer equipment, and include it in the citywide surplus inventory policy.

Status: In Progress

Recommendation #11: Review the life expectancies of critical computer systems and determine a replacement schedule and budget for the highest-priority systems and hardware.

Status: Completed

#14-06 Customer Call Handling Audit Recommendations (Issued 8/14/14)

Recommendation #1: To improve access to City services, the Administration should correct erroneous telephone numbers and links on the City website. Further, the Administration should develop policies and procedures to ensure that the City website and departmental webpages remain current and are reviewed on a regular basis by individual departments.

Status: Completed

Recommendation #2: To improve access to City services and to reduce the City's telephone call handling costs, the Administration should develop a coordinated strategy to:
a. Offer new self-service options for the City's most frequently used services by phone, online, and/or by mobile app, and
b. Establish utilization targets for new and existing self-service options, and advertise them accordingly.

Status: In Progress

Recommendation #3: To improve wait times during peak demand periods, the Customer Contact Center should:
a. Modify its staff members' duties as needed. This includes continuing call answering duty assignments to Principal Office Specialists as needed.
b. Modify its staff schedules as needed, including start, end, and break times for shifts, and scheduled time off.
c. Seek short-term staffing relief as needed. This could include engaging temporary staff and utilizing the answering service vendor.

Status: Completed

Recommendation #4: To improve their performance management, the City departments should regularly use call center statistics in analyzing past performance, expected programmatic changes,

establishing next performance objectives, examining overall performance strategies, and reviewing their staffing needs. Further, call center managers should regularly review and discuss individual call taker statistics with their staffs, and install real-time monitors where needed to provide real time customer wait time information to call takers. These performance management practices should be documented in departmental policies and procedures.

Status: In Progress

Recommendation #5: To improve performance management at call centers, the IT Department should ensure that the new telephone system enables call centers to record phone calls. The call centers should consider implementing customer surveys and should use recorded phone calls to regularly train their staff and improve customer service.

Status: Completed

Recommendation #6: To improve the customer experience in its call tree, Animal Care and Services, with assistance from the IT Department, should review and revise its call tree in accordance with best practices and:
• Make it shorter and simpler;
• Make it responsive to customer needs by removing unneeded options and ordering options meaningfully; and
• Correct the inaccurate information.

Status: Completed

Recommendation #7: To improve the customer experience in their call trees, the call centers with assistance from the IT Department should:
a. Immediately change the incorrect messages;
b. Regularly review call trees for accuracy, simplicity, and ease of use, and establish procedures to continue doing so;
c. Maintain up-to-date transcripts and flowcharts of their call trees, and establish procedures to continue doing so; and
d. Encourage callers in each call tree to use self-service options (when available).

Status: In Progress

Recommendation #8: To improve customers' voicemail experience, departments that use voicemail boxes should:
a. Develop a policy on how frequently voicemail boxes should be reviewed and how timely messages should be returned;
b. Assign their staff members primary and back-up duties to respond to voicemails, and incorporate this into their procedures;
c. Regularly review voicemail retrieval reports to ensure that voicemails are being checked;
d. Remove those voicemail boxes that will not be checked or will not be needed; and
e. Use the online interface to retrieve voicemail messages. The IT Department should ensure that the new phone system has an online voicemail interface.

Status: In Progress

Recommendation #9: To ensure accessibility of City services to non-English speakers, the Administration should clarify that the *Language Line* purchase order is available to all line departments and provide assistance to line staff on how it can be used.

Status: Completed

Recommendation #10: To ensure accessibility of City services to non-English speakers, the Administration should formulate a policy and goals that further language accessibility and provide
assistance to line departments implementing this policy.

Status: Completed

Recommendation #11: The Administration should coordinate development of an online knowledge base that enables call takers in various departments to provide accurate information to customers and minimize the number of times that a customer's call needs to be transferred.

Status: In Progress

Recommendation #12: The IT Department should work with other departments to set up automated data transfer between online service requests (web forms and mobile apps) and existing departmental work order systems. In addition, the Administration should review whether different service request systems could benefit from integration and CRM implementation.

Status: In Progress

Recommendation #13: The Administration should develop a long-term strategy to improve customer access including consideration of a centralized call center with integrated CRM.

Status: In Progress

 # 16-04 Technology Deployments: Additional Resources Timelines (Issued 3/10/16)

Recommendation #1: The Administration should establish a continuous replacement program for the City's key technology systems by:
a) Clearly defining a continuous replacement program that outlines the City's key technology systems, the end of these systems' support/useful life, the estimated cost for upgrade/replacement (if possible), etc. The program should give a clear picture of the risks the City faces by not upgrading these systems, and should be incorporated in the Status Report on Deferred Maintenance and Infrastructure Backlog;

b) Identifying and prioritizing for budget consideration an annual base level of funding required to continuously replace existing technology systems (in addition to the current process for identifying one-time funding for new technology projects); and
c) Given the City's limited resources, the CIO should determine which enterprise technology projects in the program should be prioritized based on risk, and establish a cross-departmental committee to advise on additional cross-departmental technology needs with a focus on the efficient deployment of resources to deliver the Citywide technology vision.

Status: In Progress

Recommendation #2: The Administration should ensure that Steering Committees for major technology deployments are appropriately staffed and notified of any deviations from the project concept plan and timeline, and are authorized to reallocate existing resources where needed.

Status: Completed

Recommendation #3: The Administration should prepare written project concept and communications plans for each of its upcoming major technology deployments. This document should include: project purpose, approach, necessary resources, risks and impacts of the project, and estimated timelines for each stage of the project.

Status: Completed

Recommendation #4: For major technology projects, require appointment of a qualified (preferably certified) project manager dedicated to and responsible for the entire project (including planning and deployment), with clear authority, roles, and responsibilities, and accountable to the steering committee for project progress and challenges.

Status: Completed

Recommendation #5: The Administration should build into its agreements with outside consultants a requirement to transfer responsibility/knowledge and lessons learnt during a project to internal City staff (or City Project Manager) once an implementation is complete.

Status: In Progress

Recommendation #6: Given the continuous need to replace technology systems, the Administration should hire qualified, permanent project management staff and train department staff in project management skills to develop in-house knowledge.

Status: Completed

Recommendation #7: The Administration should ensure sufficient technical resources, allocate adequate technology staff from IT and individual departments, and include these resource commitments in project concept plans.

Status: Completed

Recommendation #8: The Administration should review the overall strategic support staffing in the IT Department and ensure that its vacant positions are immediately filled. This may require salary enhancements.

Status: Completed

Recommendation #9: IT and Finance should review and update policies on technology procurement (including the purchase of PCs and monitors), make all required forms available centrally in one location, and train relevant staff on technology procurement processes.

Status: In Progress

 # 16-11 Mobile Devices: Improvements Needed to Ensure Efficient, Secure, and Strategic Deployment (Issued 12/16)

Recommendation #1: To ensure appropriate controls over City-owned mobile devices (including cellphones, smartphones, hotspots, tablets, and laptops), the Administration should require departments to label City-owned mobile devices and maintain current inventories. The inventories should include the type of device, serial number, the name and ID of the employee to whom the device is assigned, the phone number (if applicable), the date of issuance, and the date returned (if applicable).

Status: Queued

Recommendation #2: To ensure that cellphone stipends are cost-effective and reflect current technologies and the usage and needs of City employees, the Information Technology Department should work with the Finance Department to:
a) Provide guidance for departments on how to assess the cost-effectiveness of offering a stipend as opposed to issuing a City-owned device;
b) Update the eligibility criteria for stipends to reflect business need (i.e., the same criteria for City-owned devices) and delegate approval to the department level; and
c) Review and adjust the amount and structure of the City's cellphone and data stipends.
The Information Technology and Finance Departments should update City policy accordingly.

Status: Queued

Recommendation #3: To ensure cellphone stipends are terminated for employees who no longer qualify for them, the Finance Department should annually generate a list of stipend holders and send it to departments for verification that employees on the list still qualify for stipends and that they do not also have City-issued cellphones.

Status: In Progress

Recommendation #4: The Finance Department should work with the Human Resources Department to revise the Employee Exit Checklist to include a requirement that department staff notify the
Finance Department's Payroll Division to terminate a stipend when an employee transfers from the department or otherwise becomes ineligible for the stipend.

Status: In Progress

Recommendation #5: The Finance Department should:
a) Work with the City Attorney's Office to clarify City policy on the taxability of stipends and either eliminate non-taxable stipends, or provide guidance to department staff on what documentation is required for a stipend to be non-taxable.
b) If non-taxable stipends are continued, the Finance Department should review the authorization forms for employees for non-taxable stipends for required documentation to justify the non-taxable status of the stipends. Finance should then work with departments to compile any missing documents or change the status to taxable.

Status: In Progress

Recommendation #6: The Information Technology Department should develop a Mobile Device Policy to supersede the current Cellular Telephone Policy (1.7.4) to:
a) Reflect the use of all mobile devices by employees across the City, including both personal and City-owned cellphones, smartphones, tablets, hotspots, and laptops.
b) Clarify the specific duties and responsibilities of mobile device liaisons within departments who are tasked with managing such devices.
The new policy should cross-reference with the City's Information Security Policy, the Remote Access Policy, and any other relevant policies that relate to mobile devices.
Per City Council direction: develop a simpler policy covering mobile devices to replace the current 17 policies and implement appropriate cybersecurity protocols by December 2017.

Status: In Progress

Recommendation #7: To ensure consistent application of the Mobile Device Policy, the Information Technology Department should develop and provide periodic training for department liaisons on their specified administrative duties and responsibilities outlined in the policy for both City-issued and personal devices used for City business.

Status: In Progress

Recommendation #8: To address information security risks associated with mobile devices, the Information Technology Department (IT) should develop, and include in the Mobile Device Policy, guidelines and procedures for both City-issued and personally owned devices that identify:
a) The degree of access for various types of mobile devices and employee classifications in connecting to either cloud-based City services or to the City's network;

b) Any applicable support expectations by IT for personally owned mobile devices used for City business;
c) Any applicable user conditions, especially if personally owned devices may be enlisted on a mobile device management software; and
d) Any applicable IT controls over mobile devices, such as remote locking or wiping of device in case of theft or loss.
Any authorization forms, such as the Remote Access Authorization Form, should be updated accordingly.

Status: In Progress

Recommendation #9: The Information Technology Department should:
a) Develop user friendly guidelines on mobile device information security and include it as part of the Mobile Device Policy.
b) Establish periodic information security awareness trainings for all personnel who access the City's network on City-issued and personal devices.

Status: In Progress

Recommendation #10: The Administration should consider allowing short, infrequent personal calls by employees using City-owned cellphones, similar to the exception for such calls using City landline phones in the Personal Use of City Equipment policy. This exception should be included in the Mobile Device Policy.
Status: Declined

Recommendation #11: To reduce ordering turn-around and demands on staff time, we recommend the Administration:
a) Allow departments to order mobile devices (cellphones, smartphones, hotspots, tablets, and laptops) and accessories directly, through appropriate citywide purchase orders;
b) Develop a process for IT or department staff to configure devices to meet information security standards in the Mobile Device Policy.
c) Update City policy accordingly. Per City Council direction: develop a digital tool to centralize and manage orders for mobile devices across the city

Status: In Progress

Recommendation #12: To reduce ordering turn-around and demands on staff time, and to provide greater transparency and citywide inventory control, we recommend the Administration:
a) Explore tools to develop online approval form(s) for the approval of City-issued cellphones, smartphones, hotspots, tablets, and laptops, including whether the device will require remote network access, to be authorized electronically and saved in a centralized, searchable database; and
b) Revise the Procurement of Laptops and Tablets Policy (1.7.8) and reference the Remote Access Policy (1.7.3) accordingly.

Status: Queued

Recommendation #13: To facilitate departmental budgeting and business need determinations, and ensure the prudent expenditure of public funds, we recommend the Information Technology Department establish and implement procedures to regularly update the City price list to accurately reflect the current discounted prices and technical specifications of available devices, and put an explicit link to tablet pricing on its intranet site.

Status: In Progress

Recommendation #14: To address the information security risks of mobile devices, the Information Technology Department (IT) should work with departments citywide to implement Mobile Device #
Management (MDM) software citywide for the devices that pose the greatest information security risks for the City. Specifically, IT should:
a) Prioritize devices that pose the greatest information security risks for the City to be enlisted on an MDM software, and work with departments to implement MDM software citywide for those devices;
b) Establish basic minimum standards or settings within the MDM software to protect City data within the software; and
c) Either directly manage mobile devices for departments or provide administrative access for departments to manage their own devices if they have the internal capacity to manage those devices.

Status: Queued

Recommendation #15: In order to ensure that the City and/or departments control costs related to mobile device, the Information Technology Department (IT), in consultation with the Finance Department where applicable, should:
a) Administer citywide review of mobile device bills for usage and potential cost savings (e.g. zero- and low-use, plan optimization, minute and data pooling, etc.), potentially through the acquisition and utilization of telecommunications expense management software.
b) Clarify the management structure between IT and other departments in its updated Mobile Device Policy (see Recommendation #6)—including some level of departmental bill review—and provide procedures and annual trainings to responsible individuals.
c) Ensure that appropriate individuals within departments receive vendor reports and communications.
d) Ensure that all wireless service users in the City are informed of their plans' features and limitations.

Status: Queued

Recommendation #16: To support staff training, pool resources, and foster departmental innovation, the Administration should create an interdepartmental working group to serve as a forum for departments to share mobile solutions and processes, and facilitate mobile strategies across the City.

Status: In Progress

Grant Thornton Financial Statement Information Technology Findings **Attachment B**

Finding 2016-003 Informational Technology: City-Wide Information Security Program

Condition

Systems impacted: The specific information systems impacted by the below findings were provided separately to management. In addition, the Grant Thornton team met with individual system owners and points of contact to discuss the nuances of these findings which varied slightly based on information system use, architecture, and other factors.

An entity-wide information security management program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. Overall policies and plans are developed at the entity-wide level. System and application-specific procedures implement the entity-wide policy. Ongoing monitoring of control design, implementation, and operating effectiveness should also be applied so that the program includes continuous monitoring processes.

Critical within a well-established information security program are documented policies, procedures, and guidance, security roles and responsibilities identified and appropriately delineated across the organization, and performing ongoing evaluations to ensure that policies and controls intended to reduce risk are effective. Without these aspects, security controls may be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied. Grant Thornton noted weaknesses within Management's information security program; specifically:

- Management had not assigned security responsibilities associated with its decentralized control environment. For example, there was no assignment of a centralized Chief Information Security Officer ("CISO") and/or Information Security Officer(s). Further decentralized information systems did not have a Component Security Officer ("CSO") or individual that was assigned to ensure the system/location met overarching security requirements.
- Management had not finalized, published, and communicated formal policies and procedures related to information technology ("IT") control processes. Examples of draft policies and IT controls not formally documented include:

Policies in draft	Not addressed in policy
Acceptable use	Baseline security configuration setting and monitoring
Access to network and systems	Auditable event and monitoring
Anti-virus	Application change & emergency change management
Business continuity and disaster recovery	Incident response
Data classification and handling	Vulnerability scanning
Encryption	Security training
Information security	Backup and data retention
Network security	
Password	
Secure system development	

- Management did not have a processes implemented to perform continuous monitoring. Specifically, Management did not:

- Perform periodic risk and vulnerability assessments, penetration testing, continuous monitoring
  through scanning or agent-based software tools, or perform other cybersecurity activities in order to identify, track and resolve security threats.
- Perform security configuration management processes to establish and monitor platforms and
  software against best practices.

Finding 2016-004 Information Technology: Account Management, Password Configuration, Broad Privileged Access, Password Configuration, Shared Accounts, and Audit Logging/Monitoring

Condition

Systems impacted: The specific information systems impacted by the below findings were provided separately to management. In addition, the Grant Thornton team met with individual system owners and points of contact to discuss the nuances of these findings which varied slightly based on information system use, architecture, and other factors.

System authorization, access, and account management controls must be used to limit system activities to ensure legitimate use, least privilege, and segregation of duties. Access controls provide assurance that critical systems assets are safeguarded and that logical access to sensitive applications, system utilities, and data is provided only when authorized and appropriate. Further, broad or special (privileged) access privileges, such as those associated with operating /database system software, administrative accounts, and /or superusers, may allow normal controls to be overridden or otherwise circumvented. Additionally, a lack of logging and monitoring broad or privileged access may result in unusual or suspicious activity going unidentified. Grant Thornton noted the following. Grant Thornton noted Management should address the following:

Account Management

- Management did not have a process to consistently document and retain approvals related to initial authorization and ongoing changes to user's access for seven systems tested.
- Management did not perform periodic access recertification for users (including privileged users) and system accounts for 11 systems tested.
- Management did not define the timeframe in which a separated employee or contractor's access from the Network must be disabled after separation and the timeframe in which a reassigned employee's access must be reviewed and updated after reassignment.

Password Configuration

Grant Thornton noted that there was no consistent password policy City-wide for the systems identified above. As a result, we noted that password security configuration settings were not consistently aligned with best practices across the network, platforms, and devices. Specifically, we noted information systems did not meet some or all of the following:

- Minimum length requirements
- Enforce the use of alpha numeric characters
- Restrict the use of common words; and,
- Apply password expiration

In addition, we noted that information systems did not log users out after a period of inactivity or lock users out after a set number of failed password attempts.

Broad / Privileged User Accounts

- For one system tested we noted the IT team had access to the operating system and the database.
- Management did not consistently segregate system management functions such as user and system administration from functional responsibilities for seven systems tested. Further system users had IT administrative responsibilities.
- We noted that a system / tool was utilized to make direct changes to production data for a system tested. This tool enables users to bypass transactions made via the applications in the normal course of business, circumvent manual controls in place and update data directly in the database. Per discussion with Management, users require approvals before making changes to data via this tool; however; there were no systematic restrictions that required approvals prior to the updates being made.

Shared Accounts

- We noted instances where systems utilized shared accounts which negate accountability of use. Specifically a shared account was used to make direct data changes via the tool described above and to transfer information into systems.

Audit Logging and Monitoring

- Management did not log and/or monitor activities associated with privileged user accounts (e.g. system administrators, user administrators, network administrators, operators, and developers) for four systems tested. Further one system had limitations which did not allow it to log activities.
- We noted a lack of formally defined auditable events (such as privileged use, invalid password attempts, key configuration changes, or changes made directly to financial data), investigation and analysis processes.

Finding 2016-005 Information Technology: Change Management

Condition

Systems impacted: The specific information systems impacted by the below findings were provided separately to management. In addition, the Grant Thornton team met with individual system owners and points of contact to discuss the nuances of these findings which varied slightly based on information system use, architecture, and other factors.

Change management processes provide assurance that software, data, and other changes associated with information systems are approved and tested so they do not introduce functional or security risks. A disciplined process for testing, approving, and migrating changes between

environments, including into production, is essential to ensure that systems operate as intended and that no unauthorized changes are implemented.

Grant Thornton noted that Management did not have a process to consistently document and retain evidence related to change management activities including change request and approval, scheduling, initiation, testing, implementation approvals and post-implementation review for eight systems tested. In addition, we noted that City personnel do not have access to source code for one system tested, which is handled by the vendor, but were responsible for user acceptance testing and certain approvals, which were not consistently documented and retained.