City of Long Beach
Working Together to Serve

Memorandum

Date: August 20, 2015

To: Patrick H. West, City Manager

From: Laura L. Doud, City Auditor ld

Subject: **Annual Financial and Single Audits**

This memo is a follow up to the August 18 Council Agenda Item C-12 regarding the City's Annual Financial and Single Audits.

As you know, KPMG LLP performs these annual audits, and during the performance of them, KPMG personnel prepare an annual Management Letter with recommendations intended to improve internal controls that should be addressed by City Management to ensure controls are sufficient to protect City assets. Copies of the Management Letter for the past two years are attached.

As City Auditor, it is my duty to identify the significance and urgency of these issues. There are eight IT findings in the Management Letter, five of which are repeated from the prior year. In addition, six of the findings concern inappropriate user system access to key systems and processes that house critical City data.

Inappropriate user access has also been highlighted in several audits issued by my Office in recent years. Specifically:

- **Vehicle Lien Sales (March 2015)**
  It was found that a total of 15 people had access to the two highest security levels in Tow Administrator, which is the primary operating system tracking vehicle inventory and $2.75 million in annuals fees. This security level allows the employees unlimited access to edit and delete transactions. In addition, the Towing Division did not monitor, track or update access levels given to employees to ensure security levels are consistent with job duties.

- **Health Revenue Collection (January 2015)**
  The NextGen system accounts for all clinical fees billed and collected, totaling $1.7 million annually. Although the system has the ability to restrict user access down to a very detailed task level, it was not being used to ensure security was appropriately established. Division personnel were unfamiliar with access controls and relationships to system functionality. As a result, several users had inappropriate system access levels allowing them to modify and delete key transactions.

- **Building Permits (September 2014)**
  The Bureau uses the Hansen system to monitor $7 million in annual fees from building permits and inspections. We were unable to identify access levels for the 101 users of Hansen because user profiles had been modified over time with no documentation or justification for the changes. It was impossible to determine if an individual user could modify or delete data in the system, and access reports supplied by Tech Services were of no assistance. In addition, we found instances of terminated employees that were still active in Hansen and the mainframe over one year after leaving the City. The combination of not being able to determine which processes each user could perform and the large number of active users puts the integrity of the data in Hansen at risk.

- **Parks, Recreation and Marine Revenue Collection (April 2012)**
  The CLASS system is used to track a portion of the department's $6.6 million in annual fees. We found that an excessive number of employees had access to edit and delete records within the CLASS system. This prohibits management's ability to control the potential risk resulting from unauthorized or inappropriate entries. As a result, assurance cannot be provided that all monies received through the system are deposited into the City's treasury.

- **Parking Citations Collection (March 2012)**
  Parking Citation revenue, totaling $13 million annually, is managed through the AutoPROCESS software. Our audit found several instances of improper levels of system user access where employees could void, change or backdate citations without detection or supervisory review. This results in a significant fraud risk where data integrity is compromised.

- **Terminated Employees (November 2011)**
  We found that current procedures allow for significant delays in terminating former employees' network system access, thus giving individuals continued access to the City's systems for weeks and even months after termination. Policy at the time was to complete access termination with approximately 27 days, but of the 87 former employees reviewed, almost 30% did not meet this timeline.

The use of technology requires organizations to establish policies that clarify roles and responsibilities for procurement, security, usage, and maintenance of technology. These policies are usually initiated at an organization's highest level, such as your office or a steering committee, as the policies affect every department, not just IT. Without these policies or strategies, departments do not know or are confused as to their role in managing technology and securing data.

Unfortunately, the City does not have these types of policies even though my Office has consistently recommended the establishment of them. In addition, the recommendation to establish such policies was included in a 2006 Information Technology Optimization Study initiated by City management.

System access should be limited to the most restrictive authority needed by users to accomplish their duties. However, without specific guidance on assigning, monitoring, and termination of user access, the City's assets are at risk. In just the audits performed by my Office that are noted above, those systems track over $31 million in annual revenue. This does not include the revenue or confidential data at risk from systems noted in KPMG's Management Letter.

We highly recommend that you begin to address these issues immediately. Without significant effort to address the implementation in the Management Letter, KPMG could be required to perform additional testing or, in the worst case, modify their report opinion, which could adversely affect the City's credit rating.

Attachments

cc: Bryan Sastokas, Director, Technology & Innovation Department
John Gross, Director, Financial Management Department

KPMG LLP
Suite 700
20 Pacifica
Irvine, CA 92618-3391

March 28, 2014

City Council
City of Long Beach
333 West Ocean Blvd.
Long Beach, California 90081

Ladies and Gentlemen:

We have audited the financial statements of the governmental activities, the business-type activities, the discretely presented component unit, each major fund, and the aggregate remaining fund information of the City of Long Beach, California (the City), for the year ended September 30, 2013, and have issued our report thereon dated March 28, 2014. In planning and performing our audit of the financial statements of the City of Long Beach, California, in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits in *Government Auditing Standards*, issued by the Comptroller General of the United States, we considered internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing an opinion on the financial statements but not for the purpose of expressing an opinion on the effectiveness of the City's internal control. Accordingly, we do not express an opinion on the effectiveness of the City's internal control.

During our audit we noted certain matters involving internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are summarized as follows:

Net Assets

Observation

During our audit, we noted that there are no written policies or procedures in place related to the annual review of the classification of net assets as part of the City's comprehensive annual financial reporting process.

Recommendation

We recommend that the City formalize its policies or procedures for the documentation and support for the classification of net assets to ensure that the basis of the restriction is external and not an internal designation by the City.

Management's Response

The City accepts KPMG's recommendation. As part of the development of the comprehensive annual financial report, the City does perform an annual review of net position. In addition, formal policies have been written which are currently under review. The City will continue to enhance its review process and ensure that these policies and procedures for the annual review, classification and documentation of net assets are formalized.

Implementation of New Accounting Standards

Observation

During our audit, we noted that there was no detailed second review of management's implementation of new accounting standards. As a result one item was not properly reported in financial statements and changes were required to be made to prevent the statements from being material misstated.

Recommendation

We recommend that the City implement a detailed secondary review process to ensure that all aspects of the standards are appropriately implemented.

Management's Response

The City acknowledges the need to ensure that new accounting standards are appropriately implemented and will take steps to ensure that additional review processes are added as future standards are implemented.

Non-Gaap Policies

Observation

During our audit, we reviewed the City's internal control process in place to identify new non-GAAP policies and quantify the impact of new and existing non-GAAP policies to the financial statements. We noted that the City does not have a formal process in place to identify new non-GAAP policies. Furthermore, the City does not perform an analysis during the year to quantify the impact of the new and existing non-GAAP policies to the year-end financial statements. As a result of the procedures performed, we noted the City did not quantify the impact of the following non-GAAP policies:

- Recognition of revenue for several revenue sharing agreements in the year subsequent to the when the exchange transaction has taken place.

- Recognition of utility revenues when billed rather than when incurred.

- Recognition of certain items as prepaid although there is no future benefit.

- Transfers of completed construction projects are not made timely to the appropriate depreciable asset category when the asset is substantially completed and in use.

Recommendation

We recommend that the City enhance its internal controls related to the documentation and calculation of the impact of non-GAAP policies to ensure that adopted policies do not result in a material misstatement of the financial statements.

Managements Response

The City accepts KPMG's recommendation. The City continues to correct its non-GAAP policies. The City recognizes the necessity and, in conformance with the recommendations of KPMG, will adopt policies and procedures needed to ensure the recognition of revenue for revenue sharing agreements in the year when the exchange transaction has taken place. The City will continue its efforts to ensure that depreciable assets are recorded when they are placed into service. Finally, The City will seek to perform an analysis during the year to quantify the impact of the new and existing non GAAP policies to the year end financial statements.

IT General Controls – Logical Access 1

Observation

The City uses the Systems Control and Library Management, or "SCLM", system to migrate Billing and Collection (BC) and Utilities and Billing changes into the production environment. We noted that all users with access to migrate changes within SCLM have access to both develop and migrate changes. This creates a segregation of duties conflict.

Effect (or Potential Effect)

The lack of segregation of duties between the users developing the code and the users migrating the code into productions undermines the ability to detect an error and prevent migration of faulty or unauthorized code into the production environment.

Recommendation

A periodic review should be implemented to monitor SCLM program changes migrated into production to validate the application level changes are appropriate.

Management's Response

The City concurs with the recommendation. All users that should not have update access to SCLM have had their access removed. At this time, only Data Center staff can migrate changes from Test to Production in SCLM. If anyone else attempts a migration, an email is sent to Data Center staff notifying them of the failed attempt. In addition, as part of the quarterly security review, we have added a review of all SCLM changes.

IT General Controls – Logical Access 2

Observation

During our testwork over direct write and administrative access to the MS SQL Server Database Management System underlying RescueNet, we noted that 13 users that are members of the Windows network domain and responsible for the network infrastructure and communications have direct write access to the MS SQL Server Database Management System. The access is not commensurate with their job responsibilities.

Effect (or Potential Effect)

Inappropriate access to make changes to the data or database objects underlying any application could result in processing and reporting errors.

Recommendation

Direct write access to the database should be restricted to those users who require the access to fulfill their job responsibilities. In addition, monitoring controls should be implemented to log and review the users performing sensitive functions, such as "INSERT" or "ALTER" should be incorporated.

Management's Response

The City concurs with the recommendation. The access to the RescueNet Database has been reviewed and all unauthorized members have been removed. In addition the Supervisor over the DBA will review the access list on a quarterly basis to ensure that only staff whose jobs require they have access to the database can access the DB.

IT General Controls – Logical Access 3

Observation

The City uses the Financial Accounting Management Information Systems, or "FAMIS" for the General Ledger for City of Long Beach General Accounting and Financial Reporting. During KPMG's testwork over administrative access to FAMIS, we noted that a Senior Accountant has admin access to FAMIS and is responsible for reviewing the bank and journal entry reconciliations. We noted this access is inappropriate due to the lack of segregation of duties.

Effect (or Potential Effect)

The lack of segregation of duties between the business users, particularly those responsible for monitoring or reconciliation controls, and administrative access undermines the ability to detect an error or prevent an erroneous transaction from being processed.

Recommendation

Users should be provided the least amount of access required for them to fulfill their job responsibilities. In addition, user access should be segregated where possible and deemed necessary to detect errors or prevent erroneous transactions from being processed. Administative access to the applications and systems should be limited to those who are responsible for managing applications. Business users should not be granted administrative access to applications and systems as they would be able to override the business process controls.

Management's Response

The City concurs with the recommendation. Although the Senior Accountant does not perform bank reconciliations, he is responsible for reviewing bank reconciliations and journal entries. He was granted the administrative access in order to ensure that we had sufficient backup for admin staff. To ensure this audit concern has been addressed, we have removed the Senior Accountant's admin access.

IT General Controls – Logical Access 4

Observation

During our testwork over the revocation of access for terminated employees, we noted that six user IDs related to terminated employees were still active in the in-scope financial applications after two months from their dates of termination, even though the tickets to revoke their access were submitted in a timely manner. For three of the six terminated users, the user IDs were active for more than nine months.

Effect (or Potential Effect)

The untimely removal of access could result in a lack of segregation of duties as a result of a terminated employee sharing his or her password with an active employee. In turn, the lack of segregation of duties could allow a user to complete a transaction without adequate review or authorization, which could then go undetected.

Recommendation

A review of active users against the list of terminated employees should be performed by the business quarterly, if not monthly, for the in-scope financial applications to provide reasonable assurance that access is revoked for terminated employees in a timely manner. Application and system adminsitrators should be held accountable for failing to remove access in a timely manner after being notified by Human Resources of a termination.

Management's Response

The City concurs with the recommendation. TSD Management will perform monthly reviews and system access maintenance to ensure that all terminated employee' access is eliminated in a timely manner.

IT General Controls – Computer Operations 5

Observation

During our testwork over help desk operations, we noted that for 2 out of 25 Remedy tickets were not closed in a timely manner. One ticket, marked, medium, was not closed for 39 days and another, also marked medium, was not closed for 19 days.

Effect (or Potential Effect)

While in both instances, the help desk person indicated that they merely forgot to close the tickets, another ticket could go unresolved for an extended period of time and cause errors in the financial reporting process.

Recommendation

A semi-monthly, if not weekly, review of open tickets should be reviewed by the help desk supervisor to determine whether open tickets are being addressed and help desk Service Level Agreements are being met. Help desk personnel should be held accountable for not closing tickets in a timely manner, after their resolution.

Management's Response

The City concurs with the recommendation. TSD Management will review all Help Desk Tickets weekly, and ensure that completed work is closed in a timely fashion.

Automated Application Control – Payroll Transactions 6

Observation

During our testwork over access to update and modify payroll benefits, we noted the users with access to update payroll information also have access to enter and update personnel information. Users having access to update personnel information and payroll information is a segregation of duties conflict.

Effect (or Potential Effect)

The lack of segregation of duties between users with access to update personnel information and payroll information undermines the ability to detect an error or prevent an employee from being set up with erroneous information.

Recommendation

Users should be provided the least amount of access required for them to fulfill their job responsibilities. In addition, user access should be segregated where possible and deemed necessary to detect errors or prevent erroneous transactions from being processed.

As such, user access configurations should be reviewed and updated to prevent business users with access to update personnel information from having access to update payroll information.

Management's Response

The City concurs with the recommendation. Application security has been updated for Central Payroll; specifically, all Central Payroll users have been moved from the administrative group (TEC) to a group that limits their access to payroll functions (CPR).

* * * * * * *

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the City's organization gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss these comments and recommendations with you at any time.

This communication is intended solely for the information and use of management, City Council and others within the City, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

KPMG

KPMG LLP
Suite 1500
550 South Hope Street
Los Angeles, CA 90071-2629

March 27, 2015

City Council
City of Long Beach
333 West Ocean Blvd.
Long Beach, California 90081

Ladies and Gentlemen:

We have audited the financial statements of the governmental activities, the business-type activities, the discretely presented component unit, each major fund, and the aggregate remaining fund information of the City of Long Beach, California (the City), for the year ended September 30, 2014, and have issued our report thereon dated March 27, 2015. In planning and performing our audit of the financial statements of the City, in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits in *Government Auditing Standards*, issued by the Comptroller General of the United States, we considered internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing an opinion on the financial statements but not for the purpose of expressing an opinion on the effectiveness of the City's internal control. Accordingly, we do not express an opinion on the effectiveness of the City's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies, and therefore, material weaknesses or significant deficiencies may exist that were not identified. However, as discussed below, we identified a deficiency in internal control that we consider to be a material weaknesses.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. As reported in the independent auditors' report on internal control over financial reporting and on compliance and other matters based on an audit of financial statements performed in accordance with *Government Auditing Standards* issued separately, we consider deficiencies over the reporting of capital asset expenditures at the Harbor Department of the City to be a material weakness.

Although not considered to be significant deficiencies or material weaknesses, we also noted the following items during our audit, which are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are summarized as follows:

Non-GAAP Policies

Observation

During our audit, we reviewed the City's internal control process in place to identify new non-GAAP policies and quantify the impact of new and existing non-GAAP policies to the financial statements. We noted that the City does not have a formal process in place to identify new non-GAAP policies. Furthermore, the City does not perform an analysis during the year to quantify the impact of the new and existing non-GAAP policies to the year-end financial statements. As a result of the procedures performed, we noted the City did not quantify the impact of the following non-GAAP policies:

- Recognition of revenue for several revenue sharing agreements in the year subsequent to the when the exchange transaction has taken place.

- Transfers of completed construction projects are not made timely to the appropriate depreciable asset category when the asset is substantially completed and in use.

Recommendation

We recommend that the City enhance its internal controls related to the documentation and calculation of the impact of non-GAAP policies to ensure that adopted policies do not result in a material misstatement of the financial statements.

Managements Response

The City accepts KPMG's recommendation. The City continues to correct its non-GAAP policies. The City recognizes the necessity and, in conformance with the recommendations of KPMG, will continue to update our policies and procedures to ensure the recognition of revenue for revenue sharing agreements in the year when the exchange transaction has taken place. The City will continue its efforts to ensure that depreciable assets are recorded when they are placed into service. Finally, The City will seek to perform an analysis during the year to quantify the impact of the new and existing non-GAAP policies to the year-end financial statements.

Automated Application Control – Payroll Transactions

Observation

During our testwork over access to update and modify payroll benefits, we noted that ten (10) users had inappropriate access.

Effect (or Potential Effect)

The inappropriate access to update and modify payroll benefits could result in unauthorized changes to employee payroll and benefits information, and increases the risk of fraudulent transactions.

Recommendation

Users should be provided the least amount of access necessary to fulfill their job responsibilities. As such, users with access to update and modify payroll information should be limited to those responsible for processing employee payroll and benefits.

Management's Response

The City's Technology and Innovation department (TI) will establish a process that requires the Help Desk to create a task, when an employee is terminated, that is assigned to the Supervisor of the HR/Payroll system. The task will require the Supervisor to confirm that the terminated employee does not have access to HR/Payroll. If the terminated employee does have access, their access will be removed. In addition, an annual review of all employee access will be performed by the business.

IT General Controls – CC&B Administrative Access 1

Observation

The City uses the Customer Care and Billing, or "CC&B," to supports it utilities and billing operation. During our testwork over administrative access, we noted that four (4) users have inappropriate access: one intern, and three users that no longer support the CC&B application on behalf of the City.

Effect (or Potential Effect)

Administrative access allows a user to manage system configurations and the users with access to the system, including creating new users. Inappropriate administrative access to CC&B could result in the mismanagement of user access that could allow erroneous transactions to be processed without detection.

Recommendation

Users should be provided the least amount of access required for them to fulfill their job responsibilities. In addition, user access should be segregated where possible and coordinated to allow for the detection of errors or prevent erroneous transactions from being processed. Administrative access to applications and systems should be limited to those who are responsible for managing applications or not responsible for processing transactions within it.

Management's Response

TI will establish a process that requires the Help Desk to create a task, when an employee is terminated, that is assigned to the Supervisor of the CIS / MWM systems. The task will require the Supervisor to confirm that the terminated employee does not have access to CIS / MWM Systems. If the terminated employee does have access, their access will be removed. In addition, an annual review of all employee access will be performed by the business.

IT General Controls – SCLM Access

Observation

The City uses the Systems Control and Library Management, or "SCLM," system to migrate Billing and Collection (BC) and legacy Utilities and Billing changes into the production environment. We noted that the users with access to migrate changes within SCLM have access to both develop and migrate changes. This creates a segregation of duties conflict and prevent the ability to enforce controls over change management.

Effect (or Potential Effect)

The lack of segregation of duties between the users developing the code and the users migrating the code into productions undermines the ability to detect an error and prevent the migration of faulty or unauthorized code into the production environment.

Recommendation

A periodic review should be implemented to monitor SCLM program changes migrated into production to validate the application level changes were performed by appropriate personnel.

Management's Response

All users that should not have update access to SCLM were removed from access. Only the Data Center staff can migrate changes from Test to Production in SCLM. If anyone else attempts a migration an e-mail is sent to the Data Center staff notifying them of the failed attempt. As part of the quarterly security review, we have added a review of all SCLM changes.

IT General Controls – DB2 System Access

Observation

During our testwork over direct write and administrative access to the DB2 Database Management System underlying Tesseract, we noted that four users were deemed to have inappropriate access. The access is not commensurate with their job responsibilities.

Effect (or Potential Effect)

Inappropriate access to make changes to the data or database objects underlying any application could result in transaction processing and reporting errors, and unreliable data.

Recommendation

Direct write access to the database should be restricted to those users who require the access to fulfill their job responsibilities. In addition, monitoring controls to log and review those users performing sensitive functions, such as "INSERT" or "ALTER," should be implemented.

Management's Response

TI will establish a process to review access of the HR/Payroll system's Data Base on a quarterly basis. A review of all users who have access to the DB2 Database will be conducted with TI's Operations staff and the Supervisor over HR/Payroll to ensure that all access is appropriate to the users' job responsibilities.

IT General Controls – MS SQL System Access

Observation

During KPMG's testwork over direct write and administrative access to the MS SQL Server Database Management System underlying RescueNet, we noted that two users, an intern and nondatabase administrator have direct write access to the MS SQL Server Database Management System. The access is not commensurate with their job responsibilities.

Effect (or Potential Effect)

Inappropriate access to make changes to the data or database objects underlying any application could result in transaction processing and reporting errors, and unreliable data.

Recommendation

Direct write access to the database should be restricted to those users who require the access to fulfill their job responsibilities. In addition, monitoring controls to log and review those users performing sensitive functions, such as "INSERT" or "ALTER," should be implemented.

Management's Response

TI will establish a process to review access of the Zoll Ambulance Billing system's Data Base on a quarterly basis. A review of all users who have access to the database will be conducted by the DBA's and the Supervisor over the Zoll Ambulance Billing Application.

IT General Controls – Terminated User Access

Observation

During our testwork over the revocation of access for terminated employees, we noted that thirteen user IDs related to terminated employees were still active in the in-scope financial applications. Some user IDs were active more than nine months after their termination dates.

Effect (or Potential Effect)

The untimely removal of access could result in a lack of segregation of duties as a result of a terminated employee sharing his or her password with an active employee. In turn, the lack of segregation of duties could allow a user to complete a transaction without the appropriate review or authorization. As such, an erroneous transaction could processed and then go undetected.

Recommendation

A review of active users against the list of terminated employees should be performed by the business quarterly, if not monthly, for the in-scope financial applications to provide reasonable assurance that access for terminated employees is revoked in a timely manner. Application and system administrators should be held accountable for failing to revoke the access to City's applications particularly if they have failed to do so after they have received a notification of the termination from Human Resources of the termination.

Management's Response

Initially, TI Supervisors will review a list of Active Users against a list of terminated employees (from HR Payroll) to ensure that all terminated users cannot access the applications. In addition, TI will institute a long-term solution to ensure that terminated employees are removed from these systems in a timely fashion. When an employee separates from the City, a report is sent to the Helpdesk. The Helpdesk will create tasks for each system administrator to check their systems to make sure the terminated employee's access is removed.

IT General Controls – Computer Operations

Observation

During our testwork over help desk operations, we noted that for one, or 1, out of 25 Remedy tickets was not closed in a timely manner. One ticket, marked, high priority, was not closed for 63 days.

Effect (or Potential Effect)

While the help desk person may have merely forgot to close the tickets, another ticket could go unresolved for an extended period of time, which could cause errors in the financial reporting process.

Recommendation

A help desk supervisor should be responsible for performing a semimonthly, if not weekly, review of open tickets to ensure they are being addressed and help desk Service Level Agreements are upheld. Help desk personnel should be held accountable for not addressing and closing tickets in a timely manner.

Management's Response

TI will implement a process that requires the Supervisor of each group to review open Remedy Tickets on a biweekly basis. If there is a need for a ticket to remain open for an extended amount of time, the reason will be documented in the ticket.

IT General Controls – Password Configurations 7

Observation

During the testwork over the password configurations, we noted that the password parameters to the mainframe environment and the database underlying the CC&B application were not configured according to the IT policies and procedures. The mainframe environment supports the following applications: FAMIS, ADPICS, legacy Utilities and Billing, and Billings and Collections; and the database maintains the integrity of the data underlying the CC&B application. Passwords, coupled with user IDs, are used to identify and authenticate users onto these environments. Password parameters are configured to force users to employ strong passwords and prevent users from guessing a user ID's password to gain unauthorized access.

Effect (or Potential Effect)

The lack of strong passwords increases the risk of unauthorized access and the processing of unauthorized transactions. Moreover, the lack of adherence to the TI policies and procedures undermines and weakens an organization's control environment.

Recommendation

The password parameters to systems should be configured to adhere to the TI policies and procedures.

Management's Response

The Network Password Policy document refers specifically to "Network" and does not include the mainframe. However, TI will change the password length requirement for the mainframe to 8 characters. Because of system limitations, we cannot require strong passwords for the mainframe. The database IDs will also be changed to 8 characters and complex, to fall in line with AR8-29 (Network Password Policy). These changes will be gradual, the mainframe changes will be enforced as user passwords expire. AR8-29 will be updated to reflect the mainframe and database constraints.

* * * * * * *

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements and, therefore, may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the City's organization gained during our work to make comments and suggestions that we hope will be useful to you. We would be pleased to discuss these comments and recommendations with you at any time.

This communication is intended solely for the information and use of management, City Council and others within the City, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP