CITY OF SAN JOSE, CALIFORNIA
Schedule of Findings
Year Ended June 30, 2017

Section I Summary of Auditor's Results

Financial Statements

Type of auditor's report issued:	Unmodified
Internal control over financial reporting:	
Material weakness(es) identified?	Yes
Significant deficiency(ies) identified?	Yes
Noncompliance material to the financial statements noted?	None reported

Federal Awards

Internal control over major programs:	
Material weakness(es) identified?	No
Significant deficiency(ies) identified?	None Reported
Type of auditor's report issued on compliance for major programs:	Unmodified
Any audit findings disclosed that are required to be reported in accordance with 2 CFR 200.516(a)?	No

Identification of major programs:

Federal Domestic Catalog Number(s)	Name of Federal Program or Cluster
20.205, 20.219	Highway Planning and Construction Cluster
20.106	Airport Improvement Program

Dollar threshold used to distinguish between type A and type B programs:	$1,770,561
Auditee qualified as a low-risk auditee?	Yes

Section II Financial Statement Findings

Finding 2017-001 Controls over estimating loan loss reserves (Repeat Finding)

Criteria

Management is responsible for the preparation and fair presentation of the financial statements in accordance with US GAAP. This includes the design, implementation, and maintenance of internal control relevant to the preparation of financial statements that are free from material misstatement, whether due to fraud or error. Internal controls over financial statement estimates are particularly important given the important judgements inherent in making those estimates.

Condition

The City maintains a Housing Activities Fund and Low and Moderate Income Housing Asset Fund with total loans to borrowers of $ 135 million and $ 509 million, respectively, at June 30, 2017. Of those loan balances, management recorded an allowance for uncollectible loans for 47% and 55%, respectively, of the gross loan balances in these two governmental funds which are maintained on the modified accrual basis of accounting. In addition to these reserves on loan principal, management also reserved 100% or $128 million of accrued interest on these loans as uncollectable at the government-wide level which is presented on the a full accrual basis of accounting. Management's estimates for the governmental funds were made using a methodology combining an allowance for collectability risk and an allowance for present value discount at 1%. Management's methodology is documented and has been consistently applied for several years but the assumptions were not supported by evidence of incurred losses on loans such as historical results, industry data, and actual performance of individual loans or current credit quality of the borrower. Many of these traditional measures of loan losses were not tracked by the City and, therefore, were not factored into the loan loss calculation.

US GAAP outlines use of an incurred loss model when estimating loan losses. Inherent in that model is that a loss has occurred as of the financial statement date for a loan loss reserve to be accrued. In other words, expected future losses are not accrued, no matter how likely. GASB Statement 34, in particular, notes that liabilities and losses should be recognized when transactions take place. In context, this is the equivalent of the notion of "incurred" – that is, the occurrence of the transaction is the triggering event for recognition of the transaction itself. The occurrence of the transaction (the loan) would give rise to the recognition of the asset – and then the other elements of the transaction (such as losses incurred) would be recognized as they are incurred over the asset's life. GASB Statement 62 outlines the accounting for loss contingencies including impairment of receivables and underscores the notion of incurred losses for events which occur as of the financial statement date that indicate a receivable has been impaired and for which an estimate of impairment is measurable. . This incurred loss notion is made explicit in GASB 62.102 (emphasis added):

An estimated loss from a loss contingency (as defined in paragraph 96) should be accrued if both of the following conditions are met:

(a) Information available prior to issuance of the financial statements indicates that it is probable that an asset had been impaired or a liability had been incurred at the date of the financial statements. It is implicit in this condition that it should be probable that one or more future events will occur confirming the fact of the loss.
(b) The amount of the loss can be reasonably estimated.

Management was asked to provide evidence supporting the reasonableness of assumptions applied in the estimate of uncollectible loans. For example, we inquired about the policy to record a 40% reserve on certain categories of loans. While management was able to share an 11-year old point system which has evolved to a blanket 40% reserve, neither that evolved point system nor the resulting 40% had any relationship to incurred

loan losses on these loan portfolios. Therefore, management was not ultimately able to adequately support the assumptions applied even though they were able to demonstrate they had complied with their policy.

With respect to the 1% discount factor, a factor which represents 27% of the recorded reserves, management has characterized this as an opportunity cost discount in its loan loss policy (lost earnings by virtue of the monies being invested in loans instead of an investment portfolio). This same 1% was characterized differently in the footnotes to the financial statements as an adjustment for below market interest rates. Management was unable to explain how their 1% discount aligned with US GAAP but did relay on several occasions that they "make the market" on their loans and their actual interest rates of 0-6% and loan terms were market; not below market. In management's response below, however, management indicates "When this type of loan is made to developers and low income residents, the fair value of the loan receivable becomes less than its face value. In other words, this type of affordable housing loan receivable cannot be sold at its face value in the market." In this regard, we find the City's documentation and explanations about market vs. below-market interest rates and loan terms to conflict with one another and the concept of opportunity cost appears to have no support in US GAAP.

Most recently, management provided a memorandum dated November 1, 2017, which suggested the loan portfolio actually had no impaired loans but the reserve was intended to reflect the potential that as loans become due, they may be renegotiated to allow borrowers to further the housing program's objective of affordability. While we appreciate that renegotiations in future years may result in loan due date extensions or forgiveness of loans, we don't see how US GAAP would support the current accounting of future decisions and how those future decisions have any relationship to the 47% and 55% uncollectibility reserves which have evolved from the 11-year old point system.

In management's response below, however, management indicates "When this type of loan is made to developers and low income residents, the fair value of the loan receivable becomes less than its face value. In other words, this type of affordable housing loan receivable cannot be sold at its face value in the market." In this regard, we find the City's documentation and explanations about market vs. below-market interest rates and loan terms to conflict with one another and the concept of opportunity cost appears to have no support in US GAAP.

We recommend management (1) clarify what they are trying to measure with the loan reserves, (2) align what they are trying to measure with US GAAP and (3) look to actual evidence of loan impairment for reserve analyses instead of old models which have no relationship to actual impairment in the portfolio.

We were able to independently develop an estimate within an acceptable range of the recorded balance to satisfy our audit objective.

Cause
The assumptions used in developing the loan loss reserve are based on an internal policy and have not been supported by evidence of incurred losses consistent with the requirements of US GAAP.

Effect or Potential Effect
Financial statements may be misstated if key assumptions in accounting estimates are not supported by quality evidence.

Views of Responsible Officials
Management disagrees, see Management Corrective Action Plan (unaudited). We have reviewed the City's Response and, based on the Criteria, Condition, Cause and Effect discussed above, we believe our finding is still valid.

Finding 2017-002 Untimely identification of errors and lack of or inaccuracies in account reconciliations
(Repeat Finding)

Criteria
Management is responsible for the preparation and fair presentation of the financial statements in accordance with accounting principles generally accepted in the United States of America ("US GAAP"). This includes the design, implementation, and maintenance of internal control relevant to the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

Condition
The City's preparation of its Comprehensive Annual Financial Report ("CAFR") is a responsibility centralized within the Finance Department who compiles and verifies financial data, accounting estimates and US GAAP application decisions maintained by that department along with those generated by the various departments within the City's decentralized structure.

The process of preparing an accurate CAFR is complicated by the variation in levels of supervisory review, reconciliation and processing flows within the finance and other departments along with the inconsistencies in accounting background among the departments.

We noticed several areas where this challenge was apparent:

- In the City's Municipal Water Fund and Integrated Waste Management Fund, a reconciliation between the CIS subsystem and general ledger balances were not completed as a normal procedure in the year-end close. In addition, a detailed supervisory review was not performed of the reconciliation prior to being provided for audit and we discovered additional errors which led to additional adjustments in accounts receivable and revenue. For the Municipal Water Fund, correcting adjustments with a net impact of $2,034,000 were posted and an additional $423,000 was identified but not corrected to decrease accounts receivable and revenues as a result of this reconciliation. An additional $338,000 of credits were identified within the receivable subledgers that were not reclassified to liabilities, therefore we proposed an adjustment to reclassify these amounts. For the Integrated Waste Management Fund, correcting adjustments with a net impact of $610,000 were posted to increase accounts receivable and revenues as a result of this reconciliation. An additional $1,680,000 of credits were identified within the receivable subledger that were not reclassified to liabilities, therefore we proposed an adjustment to reclassify these amounts.
- Within the Special Assessments Fund and Housing Activities Fund, we identified two instances where revenue was recorded in the incorrect period and this error was not identified in a timely manner by the City. The impact of these errors was to overstate revenue in fiscal 2017 that really belong in fiscal 2016 in the amounts of $1,171,000 and $1,539,000, respectively.
- In the City's Low and Moderate Housing Fund we identified a loan which had a forgiveness clause embedded in the agreement that was not fully reserved for when it should have been in accordance with the City's policy. As such, we proposed an adjustment to increase the reserve for this loan of $1,150,000.

We recommend that Management require at least annual reconciliations of all accounts between the subsystem and the general ledger ending balances. Furthermore we recommend increased training for preparers and reviewers of journal entries and reconciliations to assist in the timely identification of errors.

Cause
Account reconciliations are not always being performed or being performed accurately. Additionally, supervisory review had not identified the lack of reconciliations or errors in those reconciliations.

Effect or Potential Effect
Deficiencies in the design or operation of reconciliation controls can lead to errors in the financial statements.

Views of Responsible Officials
Management agrees, see Management Corrective Action Plan (unaudited).

Finding 2017-003 Informational Technology: City-Wide Information Security Program (Repeat Finding)

Criteria
Internal controls over financial reporting are reliant on information technology ("IT") controls which are designed effectively. In that regard, an effectively designed IT environment is one where an organization:
(a) develops, documents, and disseminates to appropriate personnel, policies that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the policy and associated controls; and,
(b) periodically reviews and updates the current policy and procedures.

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.

Cause
Due to budget constraints and significant reductions in ITD, Management has not developed or resourced an IT governance structure and processes that appropriately support the risks and threats associated with an organization of the City's size and with the added complexities of decentralization. Furthermore, while Management was in the process of finalizing and implementing City-wide policies and procedures over IT systems, they had not developed ongoing monitoring procedures to protect the integrity of financial data, nor were appropriate processes in place in order to monitor potential security threats.

Effect or Potential Effect
A lack of formal security responsibilities, as well as, policies and procedures related to security controls increases the risk that implementation of control activities may not be consistent throughout the divisions / components within the City.

Failure to perform network security vulnerabilities and penetration assessments increases the risk that the information system's security weaknesses are not identified and investigated in a timely fashion.
Failure to implement and monitor recommended security configuration and best practice settings increases the likelihood of misconfigurations that may be exploited.

Inadequate information security frameworks may lead to lapses in security requirements and consistent implementation across decentralized locations.

This could lead to errors, data loss, inappropriate access, and other risks with the potential to impair the confidentiality, integrity, and availability of systems and data. These issues may result in unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems, which may lead to misstatements on the financial statements.

Views of Responsible Officials
Management agrees, see Management Corrective Action Plan (unaudited).

Finding 2017-004 Information Technology: Account Management, Password Configuration, Broad Privileged Access, Password Configuration, Shared Accounts, and Audit Logging/Monitoring (Repeat Finding)

Criteria

Internal controls over financial reporting are reliant on information IT controls which are designed effectively. In that regard, an effectively designed IT environment is one where an organization maintains the following:

Account Management includes the following criteria:

a. Identifies and selects the types of information system accounts needed to support organizational missions/business functions;
b. Assigns account managers for information system accounts;
c. Establishes conditions for group and role membership;
d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Requires approvals by appropriate personnel for requests to create information system accounts;
f. Creates, enables, modifies, disables, and removes information system accounts in accordance with organization-defined procedures or conditions;
g. Monitors the use of information system accounts;
h. Notifies account managers when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes;
i. Authorizes access to the information system based on a valid access authorization, intended system usage, and other attributes as required by the organization;
j. Reviews accounts for compliance with account management requirements periodically; and,
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
l. restrictions on the use of shared accounts such as defining the specific criteria that must be met in order to use a shared account and termination of the shared account credentials when members leave the group.

Password Strength the organization employs the principle of strong passwords, requiring credentials of reasonable complexity and inactivity-based log-out.

Separation of Duties the organization documents separation of duties of individuals and defines information system access authorizations to support separation of duties. Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions.

*Least Privileg*e the organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Access Restrictions for Change the organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Organizations should maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes.

Audit Events the organization:

a. Determines that the information system is capable of auditing organization-defined auditable events;
b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and,
d. Determines that the organization-defined audited events are to be audited within the information system along with the frequency of (or situation requiring) auditing for each identified event.

Audit Review, Analysis, and Reporting the organization reviews and analyzes information system audit records periodically for indications of inappropriate or unusual activity and reports findings to the appropriate personnel or role within the organization. Information security-related auditing performed by organizations can include, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP.

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 an 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.

Cause

- Management had not implemented a policy and procedures that appropriately documents account management requirements as part of their internal control framework.
- Management had not defined City-wide password security configurations. Additionally, some information systems did not have the technical capability to enforce password configuration best practices.
- Management had not defined requirements for privileged user accounts, shared accounts, logging/ monitoring, and segregation of duties in policy and procedures.

Effect or Potential Effect

Account Management

- Without formally completing or approving access requests, changes or timely terminations of access, there is an increased risk of inappropriate or unauthorized access to information systems and financial data.
- Without a periodic review of user and system accounts, there is a greater probability that an access change made in error would not be identified in a timely manner.
- Without defining the requirements around logical and physical access removal for separated or reassigned employees and contractors, there is an increased risk that access will not be removed or will not be removed in a timely manner. This access may allow inappropriate access to execute system functions. This could also lead to a license violation issue.

Password Configuration

Failure to implement recommended security settings and best practices for passwords increases the likelihood of account compromise by malicious users

Broad / Privileged User Accounts

- Failure to effectively restrict access to applications based on job function and employ adequate segregation of duties increases the risk for abuse of system privileges, fraud, and inappropriate activity without collusion.
- Direct data changes bypass system transactions and controls and therefore increase the risk of inappropriate updates to data. This may impact the organization's ability to rely on the completeness, accuracy, and validity of financial data. Further, the use of shared user accounts on a production system reduces the audit and accountability of users within the system and password security. In other words, there is no traceability of user's activity to perform these changes to production data.

Shared Accounts

Shared accounts negate accountability of use in that Management is not able to identify the user that made changes.

Audit Logging and Monitoring

Failure to maintain adequate logging and monitoring of higher risk application events and privileged access increases the risk that suspicious activities may not be identified and investigated.

This could lead to errors, data loss, inappropriate access, and other risks with the potential to impair the confidentiality, integrity, and availability of systems and data. These issues may result in unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems, which may lead to misstatements on the financial statements.

Views of Responsible Officials

Management agrees, see Management Corrective Action Plan (unaudited).

Finding 2017-005 Information Technology: Change Management
(Repeat Finding)

Criteria

Internal controls over financial reporting are reliant on IT controls which are designed effectively. In that regard, an effectively designed IT environment is one where an organization:

a. Determines the types of changes to the information system that are configuration-controlled;
b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
c. Documents configuration change decisions associated with the information system;
d. Implements approved configuration-controlled changes to the information system;
e. Retains records of configuration-controlled changes to the information system for an organization-defined time period;
f. Audits and reviews activities associated with configuration-controlled changes to the information system; and,
g. Coordinates and provides oversight for configuration change control activities through an organization-defined configuration change control element (e.g., committee, board).

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.

Cause
As part of the internal controls framework, management has not incorporated a policy and procedure to periodically monitor and review the configuration items that are migrated to production. Additionally, IT personnel did not consistently document and retain evidence related to change management activities (e.g. change request and approval, scheduling, initiation, testing, implementation approvals and post-implementation review).

Effect or Potential Effect
Without formally completing or approving change management activities for system changes, patches and modifications, there is an increased risk that change management controls will not be completed. Without effective control over changes that are migrated to the production environment, there is an increased risk that an inappropriate code change could be introduced into the production environment, potentially impacting the financial statement and related processes (i.e. cash accountability, financial reporting, etc.).

Inappropriate code change could have a negative impact on system functionality, availability, or ability to produce complete and accurate financial data. These issues may result in unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems, which may lead to misstatements on the financial statements.

Views of Responsible Officials
Management agrees, see Management Corrective Action Plan (unaudited).

Finding 2017-006 Fair value of investments held in Retirement Plans under GASB 72 (applicable to Retirement Office)
(Repeat Finding)

Criteria
Establishing and maintaining an internal control structure is an important management responsibility. To provide reasonable assurance that an entity's objectives will be achieved, the internal control structure should be under ongoing supervision by management to determine that it is operating as intended and that it is modified as appropriate for changes in conditions.

Condition
As it relates to level 3 investments (which as of June 30, 2017 were all held through one manager), management established a policy to undertake periodic validation of the amounts provided by the investment manager by engaging a third party to complete an independent valuation of material level 3 investments. However, this independent valuation was not complete in time to support the preparation of the financial statements for the year ended June 30, 2017.

Reclassification adjustments related to the GASB Statement No. 72 leveling disclosures were identified in the System's financial statements. Therefore, a detailed review of the investments in each level category was not completed at the appropriate level of precision to identify misclassifications in the different fair value categories.

Cause
The Retirement Office did not have a process in place to ensure this evaluation was completed in a timely manner.

Effect or Potential Effect
Adjustments to leveling classification.

Management should develop and implement a comprehensive policy for fair value measurements which includes, but is not limited to:

- Documentation of the techniques used to value all investment security types
- Periodic review of SOC 1 reports covering the valuation controls in place at the custodian and third party investment managers.
- Selected validation of values provided by third parties using independent pricing sources applicable to the particular security types.
- Develop and implement a comprehensive review of the investments disclosed in each levelling category compared to the pricing sources applicable to the particular security types.

Views of Responsible Officials
Management agrees, see Management Corrective Action Plan (unaudited).

CITY OF SAN JOSE, CALIFORNIA
Schedule of Findings (Concluded)
Year Ended June 30, 2017

Section III Federal Award Findings

None reported.

CITY OF SAN JOSE, CALIFORNIA
Summary Schedule of Prior Audit Findings
Year Ended June 30, 2017

Schedule of Prior Year Findings

Finding 2016-001 Risks of decentralized accounting functions, reduced finance department staffing levels

Criteria
Management is responsible for the preparation and fair presentation of the financial statements in accordance with accounting principles generally accepted in the United States of America ("US GAAP"). This includes the design, implementation, and maintenance of internal control relevant to the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

Condition
The City's preparation of its Comprehensive Annual Financial Report ("CAFR") is a responsibility centralized within the Finance Department who compiles and verifies financial data, accounting estimates and US GAAP application decisions maintained by that department along with those generated by the various departments within the City's decentralized structure.
The process of preparing an accurate CAFR is complicated by the variation in levels of supervisory review, reconciliation and processing flows within the finance and other departments along with the inconsistencies in accounting background among the departments. That coupled with employee turnover among finance functions and in the departments contributes to a challenge in maintaining an internal control environment to prepare an accurate CAFR.
We noticed several areas where this challenge was apparent:

- In the City's General Fund, we encountered an account entitled Other Liabilities with a balance of $30 million at June 30, 2016 for which there were no supporting_subsidiary ledgers to substantiate the composition of the recorded balances. In order to audit the recorded liabilities, we requested the creation of subsidiary ledgers for many of the accounts comprising the $30 million total. Once created and reviewed, , we noted a misapplication of cash receipts where amounts related to cash receipts were recorded as additions to other liabilities rather than reductions of receivables or recognized as revenue. This resulted in an overstatement of $4.1 million in other liabilities, $3.9 million in receivables and $0.2 million in revenue. See Appendix A.
- Pooled bank account reconciliation- some departmental reconciling items such as those for disbursements which had not cleared the bank (outstanding checks) were calculated as the difference between a multi-year summaries of expenses recorded and the a balance of disbursements which had not cleared the bank instead of being supported by a list of actual outstanding checks.
- Accounts receivable and advance/deposit payable, and accrued salaries and wages reconciliations- several departmental accounts receivable subsidiary ledgers provided did not agree to the general ledger, were not prepared timely and had not been through a supervisory review. Identified errors in these accounts are summarized in Appendix A.
- Schedule of Expenditures of Federal Awards- the review controls over this supplemental schedule to the financial statements did not identify errors in the expenditure data for two federal awards. The accuracy of this schedule is important to the annual federal compliance audit which uses this schedule as a basis for determining which federal programs are subject to audit in a given year.
- Loan loss reserve estimate- see following comment.

Cause
As noted in past audits and in other studies, the decentralized nature of accounting responsibilities and the turnover and staffing levels at the City contribute to the instances listed above. We understand the City has made strides in centralizing policies, providing employee training and examining efforts to hire and retain finance personnel. We commend the City for these efforts and encourage continued focus in this area and to ensure the maintenance of subsidiary ledgers and the complete reconciliation of those subsidiary ledgers to the general ledger.

Effect or Potential Effect
Errors such as those noted above are a risk in the current environment.

Status:
Some errors from 2016 did not repeat in 2017 but there were some similar errors as noted in Finding 2017-002.

Finding 2016-002 Controls over estimating loan loss reserves

Criteria
Management is responsible for the preparation and fair presentation of the financial statements in accordance with US GAAP. This includes the design, implementation, and maintenance of internal control relevant to the preparation of financial statements that are free from material misstatement, whether due to fraud or error. Internal controls over financial statement estimates are particularly important given the important judgements inherent in making those estimates.

Condition
The City maintains a Housing Activities Fund and Low and Moderate Income Housing Asset Fund with total loans to borrowers of $ 131,239 million and $ 506,215 million, respectively, at June 30, 2016. Of those loan balances, management recorded an allowance for uncollectible loans for 43% and 55%, respectively, of the gross loan balances in those funds. Management's estimates were made using a methodology combining an allowance for risk and an allowance for present value discount. Management's methodology is documented and has been consistently applied for several years but the assumptions were not supported by evidence of incurred losses on loans such as historical results, industry data, actual performance of individual loans or current credit quality of the borrower. US GAAP outlines use of an incurred loss model when estimating loan losses. Inherent in that model is that a loss has occurred as of the financial statement date for a loan loss reserve to be accrued. In other words, expected future losses are not accrued, no matter how likely. Management was asked to provide evidence supporting the reasonableness of assumptions applied in the estimate. For example, we inquired about the policy to record a 40% reserve on certain categories of loans. Management was not ultimately able to adequately support the assumptions applied even though they were able to demonstrate they had complied with their policy.
We recommend management review loan reserve methodology in the context of applicable accounting standards and enhance documentation supporting the basis for assumptions and rates applied to the loans to estimate the reserve. We were able to independently develop an estimate within an acceptable range of the recorded balance to satisfy our audit objective.

Cause
The assumptions used in developing the loan loss reserve are based on an internal policy and have not been supported by evidence of incurred loss rates consistent with US GAAP's incurred loss model.

Effect or Potential Effect
Financial statements may be misstated if key assumptions in accounting estimates are not supported by evidence.

Status:
See Finding 2017-001.

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

Criteria
Internal controls over financial reporting are reliant on information technology ("IT") controls which are designed effectively. In that regard, an effectively designed IT environment is one where an organization:
(a) develops, documents, and disseminates to appropriate personnel, policies that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the policy and associated controls; and,
(b) periodically reviews and updates the current policy and procedures.

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.

Cause
Due to budget constraints and significant reductions in ITD, Management has not developed or resourced an IT governance structure and processes that appropriately support the risks and threats associated with an organization of the City's size and with the added complexities of decentralization. Furthermore, while Management was in the process of finalizing and implementing City-wide policies and procedures over IT systems, they had not developed ongoing monitoring procedures to protect the integrity of financial data, nor were appropriate processes in place in order to monitor potential security threats.

Effect or Potential Effect
A lack of formal security responsibilities, as well as, policies and procedures related to security controls increases the risk that implementation of control activities may not be consistent throughout the divisions / components within the City.
Failure to perform network security vulnerabilities and penetration assessments increases the risk that the information system's security weaknesses are not identified and investigated in a timely fashion.
Failure to implement and monitor recommended security configuration and best practice settings increases the likelihood of misconfigurations that may be exploited.
Inadequate information security frameworks may lead to lapses in security requirements and consistent implementation across decentralized locations.
This could lead to errors, data loss, inappropriate access, and other risks with the potential to impair the confidentiality, integrity, and availability of systems and data. These issues may result in unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems, which may lead to misstatements on the financial statements.

Status:
See finding 2017-003.

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

Criteria
Internal controls over financial reporting are reliant on information IT controls which are designed effectively. In that regard, an effectively designed IT environment is one where an organization maintains the following:
Account Management includes the following criteria:

m. Identifies and selects the types of information system accounts needed to support organizational missions/business functions;
n. Assigns account managers for information system accounts;
o. Establishes conditions for group and role membership;
p. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
q. Requires approvals by appropriate personnel for requests to create information system accounts;
r. Creates, enables, modifies, disables, and removes information system accounts in accordance with organization-defined procedures or conditions;
s. Monitors the use of information system accounts;
t. Notifies account managers when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes;
u. Authorizes access to the information system based on a valid access authorization, intended system usage, and other attributes as required by the organization;
v. Reviews accounts for compliance with account management requirements periodically; and,
w. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
x. restrictions on the use of shared accounts such as defining the specific criteria that must be met in order to use a shared account and termination of the shared account credentials when members leave the group.

Password Strength the organization employs the principle of strong passwords, requiring credentials of reasonable complexity and inactivity-based log-out.

Separation of Duties the organization documents separation of duties of individuals and defines information system access authorizations to support separation of duties. Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions.

*Least Privileg*e the organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Access Restrictions for Change the organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Organizations should maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes.

Audit Events the organization:

e. Determines that the information system is capable of auditing organization-defined auditable events;
f. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

g. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and,

h. Determines that the organization-defined audited events are to be audited within the information system along with the frequency of (or situation requiring) auditing for each identified event.

Audit Review, Analysis, and Reporting the organization reviews and analyzes information system audit records periodically for indications of inappropriate or unusual activity and reports findings to the appropriate personnel or role within the organization. Information security-related auditing performed by organizations can include, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP.

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 an 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.

Cause

- Management had not implemented a policy and procedures that appropriately documents account management requirements as part of their internal control framework.
- Management had not defined City-wide password security configurations. Additionally, some information systems did not have the technical capability to enforce password configuration best practices.
- Management had not defined requirements for privileged user accounts, shared accounts, logging/ monitoring, and segregation of duties in policy and procedures.

Effect or Potential Effect

<u>Account Management</u>

- Without formally completing or approving access requests, changes or timely terminations of access, there is an increased risk of inappropriate or unauthorized access to information systems and financial data.
- Without a periodic review of user and system accounts, there is a greater probability that an access change made in error would not be identified in a timely manner.
- Without defining the requirements around logical and physical access removal for separated or reassigned employees and contractors, there is an increased risk that access will not be removed or will

not be removed in a timely manner. This access may allow inappropriate access to execute system functions. This could also lead to a license violation issue.

Password Configuration
Failure to implement recommended security settings and best practices for passwords increases the likelihood of account compromise by malicious users

Broad / Privileged User Accounts

- Failure to effectively restrict access to applications based on job function and employ adequate segregation of duties increases the risk for abuse of system privileges, fraud, and inappropriate activity without collusion.
- Direct data changes bypass system transactions and controls and therefore increase the risk of inappropriate updates to data. This may impact the organization's ability to rely on the completeness, accuracy, and validity of financial data. Further, the use of shared user accounts on a production system reduces the audit and accountability of users within the system and password security. In other words, there is no traceability of user's activity to perform these changes to production data.

Shared Accounts
Shared accounts negate accountability of use in that Management is not able to identify the user that made changes.

Audit Logging and Monitoring
Failure to maintain adequate logging and monitoring of higher risk application events and privileged access increases the risk that suspicious activities may not be identified and investigated.

This could lead to errors, data loss, inappropriate access, and other risks with the potential to impair the confidentiality, integrity, and availability of systems and data. These issues may result in unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems, which may lead to misstatements on the financial statements.

Status:
Some progress has been made among selected applications. In the aggregate a significant deficiency in internal control still exists. Refer to finding 2017-004.

Finding 2016-005 Information Technology: Change Management

Criteria
Internal controls over financial reporting are reliant on IT controls which are designed effectively. In that regard, an effectively designed IT environment is one where an organization:

h. Determines the types of changes to the information system that are configuration-controlled;
i. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
j. Documents configuration change decisions associated with the information system;
k. Implements approved configuration-controlled changes to the information system;
l. Retains records of configuration-controlled changes to the information system for an organization-defined time period;

m. Audits and reviews activities associated with configuration-controlled changes to the information system; and,

n. Coordinates and provides oversight for configuration change control activities through an organization-defined configuration change control element (e.g., committee, board).

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.

Cause

As part of the internal controls framework, management has not incorporated a policy and procedure to periodically monitor and review the configuration items that are migrated to production. Additionally, IT personnel did not consistently document and retain evidence related to change management activities (e.g. change request and approval, scheduling, initiation, testing, implementation approvals and post-implementation review).

Effect or Potential Effect

Without formally completing or approving change management activities for system changes, patches and modifications, there is an increased risk that change management controls will not be completed. Without effective control over changes that are migrated to the production environment, there is an increased risk that an inappropriate code change could be introduced into the production environment, potentially impacting the financial statement and related processes (i.e. cash accountability, financial reporting, etc.).

Inappropriate code change could have a negative impact on system functionality, availability, or ability to produce complete and accurate financial data. These issues may result in unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems, which may lead to misstatements on the financial statements.

Status:

Some progress has been made among selected applications. In the aggregate a significant deficiency in internal control still exists. Refer to finding 2017-005.

Finding 2016-006 Fair value of investments held in Retirement Plans under GASB 72(applicable to Retirement Office)

Criteria
Establishing and maintaining an internal control structure is an important management responsibility. To provide reasonable assurance that an entity's objectives will be achieved, the internal control structure should be under ongoing supervision by management to determine that it is operating as intended and that it is modified as appropriate for changes in conditions.

Condition
Grant Thornton noted that the Retirement Office had not developed a comprehensive analysis of valuation techniques applied to its level 1 investments, level 2 investments, level 3 investments and investments measured using the net asset value and did not have a clearly articulated means of demonstrating how fair values recognized in the financial statements were validated.

GASB 72 became effective for the Retirement Office for the year ended June 30, 2016 with presentation of comparable 2015 information required. GASB 72 requires new disclosures in the financial statements regarding the inputs to the valuation techniques applied in determining the fair values of the investments in the Retirement Office's investment portfolios. This necessitates analysis by management of methods used by the custodian and investment managers to measure fair value and to undertake periodic validation of the amounts provided by those parties.

GASB 72 does not change the accounting treatment for the investments, but rather defines fair value and the way it is to be measured and recognized in financial statements, establishes new disclosure requirements and sets new expectations regarding related documentation. Historically the standard practice had been limited to accepting values provided by third parties on the basis of an expectation that they had effective controls over fair value measurements.

Cause
The Retirement Office did not have a process in place for fully implementing this new accounting standard.

Effect or Potential Effect
Clear support was not initially provided demonstrating management's understanding of valuation techniques and the related validation of amounts provided by the custodian and investment managers.

Management should develop and implement a comprehensive policy for fair value measurements which includes, but is not limited to:

- Documentation of the techniques used to value all investment security types
- Periodic review of SOC 1 reports covering the valuation controls in place at the custodian and third party investment managers.

Selected validation of values provided by third parties using independent pricing sources applicable to the particular security types.

Status:
See Finding 2017-006

Finding 2016-007 Procurement under Federal Uniform Guidance

Federal Award: WIA/WIOA Cluster, CFDA 17.258, 17.259, 17.277, 17.278

Federal Award: Airport Improvement Program, CFDA 20.106

Criteria
Pursuant to the U.S. Office of Management and Budget's ("OMB") Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards("Uniform Guidance") in 2 CFR 200, recipients of Federal awards must implement the policies and procedures applicable to Federal awards effective December 26, 2014 unless different provisions are required by statute or approved by OMB. For the procurement standards in 2 CFR 200.317 – 200.326, Federal award recipient entities may continue to comply with the procurement standards in previous OMB guidance for two additional fiscal years after this part goes into effect. If a Federal award recipient chooses to use the previous procurement standards for an additional two fiscal years before adopting the procurement standards in this part, the Federal award recipient must document this decision in their internal procurement policies.

Condition
We noted that the City did not document any decision to continue to use the procurement standards in the previous OMB guidance for an additional two fiscal years subsequent to the December 26, 2014 effective date of the new Uniform Guidance rules.

Context
The City had the ability to defer implementation of the new Uniform Guidance procurement rules outlined in 2 CFR 200 for two years but did not formally document the decision and it was unclear which rules the City was operating under for procurements on Federal grants and contracts after the December 26, 2014 implementation date.

Questioned Costs
$0

Effect
The City did not comply with the specific requirements of Uniform Guidance with respect to documenting its procurement policies.

Cause
Procurement personnel neglected to document the deferral of the implementation of the new rules.

Recommendation
We recommended and the City has since documented its decision to defer adoption of the new procurement standards until July 1, 2017.

Status:
Remediated

Finding 2016-008 Evaluating controls over third party service providers

Criteria
Management is responsible for the preparation and fair presentation of the financial statements in accordance with US GAAP. This includes the design, implementation, and maintenance of internal control relevant to the

preparation of financial statements that are free from material misstatement, whether due to fraud or error. Effective internal controls include the monitoring of third party service providers who process transactions on behalf of the City.

Condition
The City engages third party service providers for a variety of services including the valuation of investments held in defined contribution pension plans (Voya) and the collection and processing of claims information for workers compensation (Athens), among others. The use of third party providers requires an evaluation of the adequacy of controls at those providers and at design and assessment of adequacy of the City's controls around the use of third party information in financial reporting. This assessment is critical to establishing that third party information is materially correct and adequately supports the accounts and balances on which such information relies.

In order to perform this assessment, the City should request and evaluate the Service Organization Control ("SOC") reports of third party providers. A SOC report is an independent auditors report obtained by service providers which reflects the results of reviews and/or testing of the service providers' internal control environment relevant to the processes outsourced to those providers. The reports provide information to users to evaluate and mitigate risks around the use of such providers and the transmission and receipt of information important to supporting financial accounts and balances and provide recommended user control considerations for application in the user's (City's) own internal control environment.

SOC reports were available for the third parties valuing investments in the defined contribution pension plans and processing workers' compensation claims but were not collected, read or analyzed by the City.

Cause
The City was unaware of the existence of the SOC reports.

Effect or Potential Effect
The City may not be aware of reported internal control deficiencies at third party providers or fail to identify important controls which should be in place at the City as it liaises with those third parties.

Status:
Remediated

Finding 2016-009 Financial Reporting Controls

Criteria
Management is responsible for the preparation and fair presentation of the financial statements in accordance with US GAAP. This includes the design, implementation, and maintenance of internal control relevant to the preparation of financial statements that are free from material misstatement, whether due to fraud or error. Internal controls over financial reporting should include a documented reconciliation between the general ledger and the formal financial statements to show a roadmap of any top-level adjustments, reclassifications and any other post-closing journal entries made to convert from one presentation to the other.

Condition
The preparation of the financial statements requires mapping of trial balance accounts to the financial statement line items and disclosures. The City uses a software application to map the trial balance to financial statements for all funds except the Wastewater Fund. For the Wastewater Fund, the City applies a highly manual, undocumented process to map the trial balance to financial statements. Post-closing, top-sided and reclassification entries could also not be easily mapped to the financial statement presentation. Further, there was no indication of any supervisory review of the accuracy and consistency of the mapping applied.

We incurred a significant amount of time reconstructing the process of mapping in order to support our audit objective.

We recommend that management fully document the complicated mapping process for this fund in the future and ensure supervisory review of this process.

Cause
There was no policy to require documentation or supervisory review of the mapping of this fund from the general ledger to the financial statements.

Effect or Potential Effect
The lack of a documented reconciliation or supervisory review could result in an error in the financial statements.

Status:
Remediated