CITY OF SAN JOSE

Report to Those Charged with Governance

For the Year Ended
June 30, 2016

CITY OF SAN JOSE

City Council For the Year Ended June 30, 2016

Table of Contents

Management and City Council
City of San José, California

Grant Thornton LLP
150 Almaden Boulevard, Suite 600
San Jose, CA 95113-2015

T 408.275.9000
F 408.275.0582
www.GrantThornton.com

Ladies and Gentlemen:

In connection with our audit of the financial statements of the governmental activities, the business-type activities, each major fund, and the aggregate remaining information, which collectively comprise the City's basic financial statements ("financial statements") of City of San Jose, California (collectively, the "City"), as of and for the year then ended June 30, 2016, auditing standards generally accepted in the United States of America ("US GAAS") and Government Auditing Standards issued by the Comptroller General of the United States (GAGAS) require that we communicate the following information related to our audit to management and City Council (hereinafter referred to as "those charged with governance").

In addition to the City's basic financial statements, we audited and separately reported on the financial statements of the Successor Agency to the Redevelopment Agency of the City of San Jose ("SARA"), the Norman Y. Mineta San Jose International Airport, the Police and Fire Department Retirement Plan, the Federated City Employees' Retirement System, the San Jose –Santa Clara Clean Water Financing Authority, the Parks and Recreation Bond Projects Fund, the Library Parcel Tax Special Revenue Fund, the Neighborhood Security Bond Projects Fund and the Library Parcel Tax Special Revenue Fund as of and for the year ended June 30, 2016.

Responsibilities

Our responsibilities

We are responsible for:

- Performing audits under US GAAS of the financial statements prepared by management, with your oversight
- Forming and expressing opinions about whether the financial statements are presented fairly, in all material respects in accordance with US GAAP
- Forming and expressing an opinion about whether certain supplementary information is fairly stated in relation to the financial statements as a whole
- Communicating specific matters to you

An audit provides reasonable, not absolute, assurance that the financial statements do not contain material misstatements due to fraud or error. It does not relieve you or management of your responsibilities. Our respective responsibilities are described further in our engagement letters including communications required by US GAAS, GAGAS and the Office of Management and Budget's Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards ("Uniform Guidance"). We have also communicated information about our audit plan to the City in our communication from August 2, 2016.

Grant Thornton

Those Charged with Governance and Management responsibilities

Those Charged with Governance (City Council):

- Overseeing the financial reporting process
- Setting a positive tone at the top and challenging the City's activities in the financial arena
- Discussing significant accounting and internal control matters with management
- Informing us about fraud or suspected fraud, including its views about fraud risks
- Informing us about other matters that are relevant to our audit, such as:

  - Objectives and strategies and related business risks that may result in material misstatement
  - Matters warranting particular audit attention
  - Significant communications with regulators
  - Matters related to the effectiveness of internal control and your related oversight responsibilities
  - Your views regarding our current communications and your actions regarding previous communications

Management:

- Preparing and fairly presenting the financial statements in accordance with US GAAP
- Designing, implementing, evaluating, and maintaining effective internal control over financial reporting
- Communicating significant accounting and internal control matters to those charged with governance
- Providing us with unrestricted access to all persons and all information relevant to our audit
- Informing us about fraud, illegal acts, significant deficiencies, and material weaknesses
- Adjusting the financial statements, including disclosures, to correct material misstatements
- Informing us of subsequent events
- Providing us with certain written representations
- Complying with laws and regulations on federal awards and designing effective internal control to ensure compliance
- Complying with contractual agreements that are the subject matter of compliance attestation examinations

Audit Scope

Materiality

Essentially, materiality is the magnitude of an omission or misstatement that likely influences a reasonable person's judgment. It is based on a relevant financial statement benchmark. We believe that total assets is the appropriate benchmark for the major funds of the City, excluding the General Fund. We believe that total revenue is the appropriate benchmark for the General Fund. Financial statement items greater than materiality are in scope. Other areas less than materiality may be in scope if qualitative factors are present (for example, related party relationships or transactions and fraud risk). Materiality for the major programs in the Federal Uniform Guidance compliance audit was benchmarked on expenditures charged to the major programs.

Change in Audit Plan

In the course of auditing the $142 million worker's compensation liability, management did not provide access to review claim files for a sample of claims citing concerns about violating State of California privacy laws. In order to proceed with the audit, we and the City agreed to have the City's internal auditor conduct certain limited audited procedures on our behalf. Our engagement letters were amended to reflect this change in the audit plan.

Quality of accounting practices

Accounting policies

Accounting policies are consistently and appropriately applied. The significant accounting policies are disclosed in the financial statements.

Accounting estimates

We believe that the following item represents particularly sensitive accounting estimates - allowance for receivables, allowance for loan losses, accruals for worker's compensation and other self-insured liabilities, fair value of investments, useful lives of depreciable assets, accrual of compensated absences, and pension and defined benefit obligations. We are satisfied as to the reasonableness of management's current judgment regarding such estimates in the context of the financial statements taken as a whole, based on our knowledge of management's process for making such judgment, inquiry of management and others regarding such matters, and other audit procedures applied during the engagement.

Management consultation with other independent accountants

In some cases, management may decide to consult with other accountant about auditing and accounting matters to obtain a second opinion. If a consultation involves application of an accounting principle to the City's financial statements or a determination of the type of auditor's opinion that may be expressed on those financial statements, our professional standards require the consulting accountant to communicate with us to determine that the consultant has all the relevant facts. To our knowledge, there were no such consultation with other accountants.

Disagreements with Management

For purposes of this letter, a disagreement with management is a financial accounting, reporting, or auditing matter, whether or not resolved to our satisfaction, that could be significant to the financial statements or the auditor's report. We are pleased to report no such disagreements arose during the course of our audit.

Internal Control Matters

In connection with our audit of the governmental activities, the business-type activities, the aggregate discretely presented component units, each major fund, and the aggregate remaining fund information of City of San Jose, California (the "City") as of June 30, 2016 and for the year then ended, auditing standards generally accepted in the United States of America ("US GAAS") require that we advise City Council (hereinafter referred to as "those charged with governance") of the following internal control matters identified during our audit.

Our responsibilities

Our responsibility, as prescribed by US GAAS, is to plan and perform our audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether due to fraud or error. An

audit includes consideration of internal control over financial reporting (hereinafter referred to as "internal control") as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our 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 express no such opinion on internal control effectiveness.

Identified deficiencies in internal control

We identified the following internal control matters that are of sufficient importance to merit your attention.

Significant deficiencies

Our consideration of internal control was also not designed to identify deficiencies in internal control that, individually or in combination, might be significant deficiencies; therefore, significant deficiencies may exist that were not identified. 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.

We consider the following identified control deficiencies to be significant deficiencies.

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.

Management response:
The City believes the control deficiencies identified during the audit are not significant. During the audit, the total amount of potential adjustments ($10.8 million) identified for fiscal year 2015-2016 was smaller than the total adjustments ($20.7 million) for fiscal year 2014-2015. For the General Fund, the total adjustments were $8.3 million for fiscal year 2015-2016, while the adjustments were $16.0 million for fiscal year 2014-2015.

All of the potential adjustments were deemed immaterial by Grant Thornton and no adjustments were required to this year's financial statements. Additionally, the listing and detailed discussion of adjustments are materially insignificant in the entirety of the City's financial statements.

The City will address the following areas pointed out by Grant Thornton:

- Other Liabilities: The Finance Department will work with departments to ensure a regular reconciliation of subledgers for Other Liabilities are reconciled to the general ledger.

- Pooled bank account reconciliation: The Finance Department will work with departments to ensure that a list of outstanding checks is submitted to the Finance Department to support the outstanding checks reported in the City-wide cash bank reconciliations.
- The Finance Department will continue to encourage departments to prepare account reconciliations and ensure these accounts reconcile with general ledger balances, and to provide proper review of schedules including Expenditures of Federal Awards.

The City continues to make modest investments in addressing the challenges associated with the City's decentralized accounting functions, reduced staffing levels in the Finance Department, high staff turnover in certain critical job classifications and increased complexities associated with financial accounting and reporting. For example, in addition to utilizing additional modules of a new financial reporting software, the Finance Department strategically assigns critical areas of the complex accounting and financial areas to more seasoned employees, when available. In recruiting new employees, the Finance Department continues to evaluate, align, and provide consistency in the experience of professionals throughout the City by working with Human Resources and partners with other departments through active participation in the recruitment of new employees who will be assigned to accounting and fiscal functions throughout the City.

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.

Management Response:
The City believes that the methodology for loan loss reserve is acceptable under GASB rules. The City has used this methodology for twenty seven years and this methodology has withstood internal and regular external audits. In addition, Grant Thornton was able to recalculate the loan loss reserve and Grant Thornton's methodology produced a result similar to the City's loan loss reserve. The City is committed to performing a regular and ongoing evaluation of the City's affordable housing loan portfolio and maintaining formal documentation of the loan loss reserve methodology including evidence-based assumptions and review of peer agencies.

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 Information Technology Department (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.

Management Response:
The audit identifies significant resource needs that Management concurs with. In August 2016, the City recognized increasing cybersecurity risks affecting its functions and operations. The City is in the process of developing its first dedicated Cybersecurity function to confront emerging risks associated with data exfiltration, malware, social engineering, denial-of-service attacks, and advanced persistent threats. Management recognizes the importance of information and systems security to the organization's fiscal status, insurability, compliance with laws and regulations, and overall wellbeing.

The City is currently building the cybersecurity program around the NIST Cybersecurity Framework. The model addresses the following critical functions to adequately address the security of information and electronic assets: Identify, Protect, Detect, Respond, Recover. Policies in draft are being modified to include feedback from this audit and the work on the Office of the City Auditor. Management will focus more heavily on the Identify and Protect functions initially per the recommendations of this audit.

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:

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

<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.

Management Response:

Individual items are accurate and Management concurs with the Audit Criteria. Nonetheless, overall risk of occurrence and impacts of occurrence are most probably minor in the context of financial reporting—e.g. limits on network access restrict non-employee access; database edits would cause anomalies that would evidence elsewhere in reporting; small staff sizes extant in the City demands some roles be combined; and no evidence has emerged of any malicious activity.

Management agrees with the need to develop mature Access Control processes and Awareness and Training.

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:

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.

Management Response:
Comments are accurate and Management concurs with the Audit Criteria. However, overall risk of occurrence and impacts are most probably minor in the context of financial reporting—e.g. change controls occur on a technical level across system and application teams for major changes; backups are available in the event a critical restore of data is required; erroneous changes would likely cause data anomalies elsewhere in financial reports that would trigger review; and no evidence has emerged of any malicious activity.

Management agrees with the need to develop mature Information Protection Processes and Procedures and Awareness and Training. The City will commence implementation of appropriate tools, controls, and training of essential personnel.

Finding 2016-006 Fair value of investments held in Retirement Plans under GASB 72(applicable to Office of Retirement Services and reported for Information Purposes)

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.

Office of Retirement Services Response:
As part of this year's financial statement preparation process, the Office of Retirement Services (ORS) investment staff documented how manager valuations and their respective valuation policies are utilized internally. In addition staff documented how the Plans' custodian, and general consultants, obtain and report valuations on behalf of the Plans. It is staff's intention to have these valuation procedures imbedded into the formal manager due diligence process currently being documented by an external third party. The formal manager due diligence process will also be formatted into the recent implementation of a research management system including the archiving of manager valuation policies.

In addition to the changes that the Investments team will be implementing in the future, accounting staff of the ORS be obtaining every single Schedule K-1 and audited financial statements for each applicable investment. Then an analysis similar to what was done this year will be completed and compared to the unaudited statements provided by the investment manager to provide assurance and comfort over the valuation that is provided.

Control deficiencies

A deficiency in internal control ("control deficiency") 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.

We identified the following control deficiencies:

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.

Management Response:
The City documented its decision to defer the implementation of the Uniform Guidance with respect to its procurement policies and is working on updating its procurement policies to meet the requirements of the new Uniform Guidance rules.

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 who 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.

Management Response
The City will evaluate its resources and develop a plan including taking an inventory of the City's third party service providers, requesting and reviewing SOC 1 reports for each service provider, and assess any deficiencies in their internal controls.

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.

Management Response:
The preparation of the Wastewater Fund is a documented process, however due to its complexity, the whole process of mapping the general ledger to the financial statements may not be evident to someone new reviewing the process. As a result of this recommendation, the City has since developed another schedule that shows the "bridge" between funds, the general ledger to financial statements, and post close entries. The new schedule has been reviewed by an Accounting Supervisor in the Environmental Services Department (ESD) and prior to the end of the current fiscal year, the Finance Department Accounting staff will review ESD's documentation to assist in the audit process next year.

Grant Thornton

Status of Prior Control Deficiency Comments

2015-001- Risk Assessment of Internal Controls Over the Financial Reporting Process

Condition/Effect:
Between 2004 and 2015, the City reduced its budgeted positions by 25 percent. This reduction and displacement of staff through the Civil Service Rules resulted in a significant disruption in the City's ability to maintain appropriate financial internal controls.

In addition, prior auditors, MGO, noted that the City continues to experience turnover in key finance positions throughout the City without experienced personnel to step into the financial reporting role.

Recommendation:
The City will need to continue to evaluate the experience of professionals throughout the City assigned to key roles in the preparation of financial statements to ensure that the most experienced professionals are responsible for the higher risk areas in the financial presentation and that there is a robust supervision and review process over those professionals with developing experience. The City should develop a robust succession plan to prepare for planned and unplanned absences of key finance professional throughout the City.

Status:
In progress. See current year comment, 2016-001.

2015-002- Workers' Compensation Claims Control

Condition/Effect:
During the testing performed by prior auditors, MGO, they noted 40 exceptions in active case files out of a population of 362 active case files:

- One claim file did not include the claimant certification for the benefits.
- Four claim files did not include review and approval of the workers' compensation reserve computations in excess of the adjuster's authority levels.
- One claim file did not include review and approval of the workers' compensation claim.
- One claim file showed a reserve amount in the claims database that was different from the supporting documentation.

Recommendation:
The City should evaluate the effectiveness of its current control processes to ensure that they are operating as designed to safeguard assets and meets its financial reporting requirements.

Status:
Implemented.

2015-003- Application of the Availability Criterion for Revenue Recognition

Condition/Effect:
During the audit, prior auditor's, MGO, noted that the City did not consistency apply the availability criterion in its governmental fund financial statements and overstated revenues in its governmental funds by $1.5 million.

Recommendation:
MGO recommended that the Finance Department continue training financial preparers in the other departments on the application of the availability criterion. In addition, the Finance Department should establish a review process at the end of the 60-day period to compare governmental department's significant revenue year-end accruals with remittances. Departments that show significant variances in collections of receivables should provide documentation supporting the validity and propriety of the revenue recorded.

Status:
Implemented.

2015-004- Utility Billing System Rates

Condition/Effect:
During the audit, prior auditor's, MGO, noted a charge rate based on the zone allocation in one of the of 25 water service customers selections tested. This resulted in a credit of $5,100 to a customer dating back to 2012.

Recommendation:
MGO recommended that the City evaluate the design of its current procedures to ensure that charge rates and zones recorded in its utility billing system accurate produces current billings to customers.

Status:
In July 2015, the City retired the Integrated Billing System and implemented a new system, "CIS Infinity." As part of the conversion and implementation plan, a widespread data cleanup effort has taken place, wherein a large part of the emphasis has been placed on remediation of previously identified issues, including ensuring all rates within the new system are accurate and correct.

The City's written response (Management's Response) to the internal control matters identified herein have not been subjected to our audit procedures and, accordingly, we express no opinion on it.

* * *

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

We would like to thank City management and staff for the cooperation extended to us during the course of our engagement.

Very truly yours,

GRANT THORNTON LLP

Grant Thornton LLP

December 1, 2016
San Jose, California

Appendix A- Unrecorded Misstatements Identified during 2016 Audit

	Fund	Acct. Description	Debit	Credit
1	Housing Fund	Intergovernmental Revenue	54,638	
	Housing Fund	Housing Receivable		(54,638)
	To adjust AR to true amount collected.			
2	General Fund	Other Liabilities	1,870,720	
	General Fund	Cash		(1,870,720)
	Waste Water	Cash	974,636	
	Waste Water	Accounts Receivable		(974,636)
	Muni Water	Accounts Receivable	63,215	
	Muni Water	Revenue		(63,215)
	Non-Major Govt Funds	Cash	896,084	
	Non-Major Govt Funds	Accounts Receivable		(896,084)
	To correct miscoded payments coded to Other Liabilities and differences between subledger and AR account.			
3	General Fund	Salary Expense	2,288,511	
	General Fund	Accrued Salaries		(2,288,511)
	To increase salary accrual to amount actually paid out for P14.			
4	General Fund	Other Liabilities	2,204,727	
	General Fund	Cash		(277,541)
	General Fund	Revenue		(174,270)
	General Fund	Accounts Receivable		(1,752,916)
	Airport	Cash	277,541	
	Airport	Accounts Receivable		(277,541)
	To apply payments sitting in suspense account at year end.			
5	Muni Water	Accounts Receivable	138,121	
	Muni Water	Revenue		(138,121)
	To record additional days of muni water revenue not accrued for.			
6	Muni Water	Deposits Payable	369,289	
	Muni Water	Cash		(369,289)
	General Fund	Cash	369,289	
	General Fund	Unrestricted Net Position		(369,289)
	To release a deposit that is past the statute of limitations.			

Unrecorded Misstatements Identified during 2016 Audit

	Fund	Acct. Description	Debit	Credit
7	General Fund	Unearned Revenue	1,536,826	
	General Fund	Accounts Receivable		(1,536,826)
	To reverse unearned revenue for which cash has not been received.			
8	Police and Fire	Net Depreciation in FV	2,613,455	
	Police and Fire	Investment		(2,613,455)
	To reverse the foreign exchange conversion on the investment as the investment is held in USD not EUR.			
9	Federated	Investments	1,768,541	
	Federated	Net Appreciation in FV		(1,768,541)
	To record the investment at fair value as management received the third party statement after closing the books.			
10	Federated	Employer Contributions - Tier 1	3,811,000	
	Federated	Net Position		(3,811,000)
	To reverse Tier 1 defined benefit contribution associated with FY 15 payroll accrual that was properly not recorded.			
11	Airport	Terminal Rent	2,499,203	
	Airport	Accounts Receivable		(2,499,203)
	To account for estimate of adjustment to terminal rent.			

Reversals of Prior Year Passed Adjustments

1	General Fund	Unrestricted Net Position	2,586,000	
	General Fund	Sales Taxes Revenue		(2,586,000)
	To adjust for additional revenue incorrectly recognized in prior year.			
2	General Fund	Unrestricted Net Position	2,826,000	
	General Fund	Expenditures		(2,826,000)
	To adjust for additional taken in current year that should have been recorded in prior year.			
3	Muni Water	Charges for Services	2,036,000	
	Muni Water	Unrestricted Net Position		(2,036,000)
	To reverse the impact of prior year unbilled revenue.			

Passed Disclosure Adjustment

Note D-Capital Assets- Transfers related to Capitalized Leases should have been adjusted in the prior year however is showing as current year activity for the Governmental and Business-type Activities in Footnote D. Presentation impact only.