CITY OF SAN JOSE

Report to Those Charged With Governance

For the Year Ended June 30, 2019

CITY OF SAN JOSE
Report to Those Charged With Governance
For the Year Ended June 30, 2019

Table of Contents

Page(s)

Certified Public Accountants

Honorable Mayor and City Council

City of San José, California

Ladies and Gentlemen:

In planning and performing our audit of the financial statements of the governmental activities, the business-type activities, each major fund, and the aggregate remaining fund information, of the City of San José, California (City), as of and for the year ended June 30, 2019, in accordance with auditing standards generally accepted in the United States of America, we considered the City's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the City's internal control. Accordingly, we do not express an opinion on the effectiveness of the City's internal control.

In addition to the City's financial statements, we audit and separately report on the financial statements of the Successor Agency to the Redevelopment Agency of the City of San José, the Norman Y. Mineta San José International Airport, the San José –Santa Clara Clean Water Financing Authority, the Parks and Recreation Bond Projects Fund, the Library Parcel Tax Special Revenue Fund, the Library Parcel Tax Special Revenue Fund, the Pedestrian/Bicycle Facilities Grant, and the City of San José Deferred Compensation Plans as of and for the year ended June 30, 2019.

We did not audit the financial statements of the City of San José Federated City Employees' Retirement System and the City of San José Police and Fire Department Retirement Plan (collectively, "the Pension Trust Funds"). Those statements were separately reported on by other auditors and the required communications related to those audits were presented to the respective Retirement Boards.

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

A *deficiency in internal control* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A *material weakness* is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. We consider finding 2019-001 to be a material weakness.

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 finding 2019-002 to be a significant deficiency.

The City's written responses to the findings and recommendations identified are described in the Schedule of Findings and Management Responses section. The City's responses were not subjected to the auditing procedures applied in our audits of the financial statements. We did not audit the City's responses and, accordingly, we express no opinion on them. In addition, we would be pleased to discuss the recommendations in further detail at your convenience, to perform any additional study of these matters, or to assist you in implementing these recommendations.

Professional standards require that we provide you with information about our responsibilities under generally accepted auditing standards, *Government Auditing Standards* and the Uniform Guidance, as well as certain information related to the planned scope and timing of our audit. We have communicated such information in our audit plan to the City dated July 18, 2019. Professional standards also require that we communicate to you the information related to our audits discussed on pages 3 through 6.

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

This communication is intended solely for the information and use of the Mayor, City Council, Public Safety, Finance & Strategic Support Committee, City management, and others within the organization, and is not intended to be, and should not be, used by anyone other than these specified parties.

Macias Gini & O'Connell LLP

Walnut Creek, California
November 14, 2019

REQUIRED COMMUNICATIONS

I. Significant Audit Findings

Qualitative Aspects of Accounting Practices
Management is responsible for the selection and use of appropriate accounting policies. The significant accounting policies used by the City are described in Note I to the City's basic financial statements. As described in Note I.E. to the financial statements, the City changed accounting policies related to the following:

- **GASB Statement No. 83 – *Certain Asset Retirement Obligations***
  This statement addresses accounting and financial reporting for certain asset retirement obligations (AROs). An ARO is a legally enforceable liability associated with the retirement of a tangible capital asset. This statement did not have any effect the City's financial statements.

- **GASB Statement No. 88 – *Certain Disclosures Related to Debt, including Direct Borrowings and Direct Placements***
  This statement defines debt for purposes of disclosure in notes to financial statements as a liability that arises from a contractual obligation to pay cash or other assets that may be used in lieu of cash in one or more payments to settle an amount that is fixed at the date the contractual obligation is established. This statement requires that additional essential information related to debt be disclosed in the notes to financial statements, including unused lines of credit; assets pledged as collateral for the debt; and terms specified in debt agreements related to significant events of default with finance-related consequences, significant termination events with finance related consequences, and significant subjective acceleration clauses. This statement also requires that existing and additional information be provided for direct borrowings and direct placements of debt separately from other debt. The application of this statement added additional disclosures to Notes III.F. and IV.C. to the financial statements.

We noted no transactions entered into by the City during the year for which there is a lack of authoritative guidance or consensus. All significant transactions have been recognized in the financial statements in the proper period.

Accounting estimates are an integral part of the financial statements prepared by management and are based on management's knowledge and experience about past and current events and assumptions about future events. Certain accounting estimates are particularly sensitive because of their significance to the financial statements and because of the possibility that future events affecting them may differ significantly from those expected.

The most sensitive estimates affecting the financial statements were:

- Measurement of investments at fair value
- Estimated allowance for losses on accounts receivable
- Estimated allowance for losses on loans receivable
- Estimated valuation of property held for resale
- Accrual and disclosure of self-insurance claims liabilities
- Depreciation estimates for capital assets, including depreciation methods and useful lives assigned to depreciable property
- Accrual of compensated absences

- Valuation of net pension liability, pension expense, and pension-related deferred outflows and inflows of resources
- Valuation of net OPEB liability, OPEB expense, and OPEB-related deferred outflows and inflows of resources
- Accrual and disclosure of pollution remediation obligations

Management's estimates were based on the following:

- The City's investments are accounted for in accordance with the provisions of GASB Statement No. 72, *Fair Value Measurement and Application*, and accordingly, its fair value measurements are categorized within the fair value hierarchy established by the standard. The following levels indicate the hierarchy of inputs used to measure fair value and the primary valuation methodologies used for financial instruments measured at fair value on a recurring basis:
    - Level 1 – Investments whose values are based on quoted prices (unadjusted) for identical assets in active markets that a government can access at the measurement date.
    - Level 2 – Investments whose values are based on inputs – other than quoted prices including prices included within level 1 – that are observable for an asset, either directly or indirectly.
    - Level 3 – Investments whose values are based on unobservable inputs for an asset and may require a degree of professional judgment.
- Estimated allowance for losses on accounts receivable was based on historical experience.
- Estimated allowance for loans receivable is comprised of an allowance for risk and an allowance for present value discount. The allowance for risk was based on the consideration of the changes in the portfolio character, evaluation of current economic conditions and management's estimate regarding the likelihood of collectability based on loan provisions and collateral. The allowance for present value discount gives recognition to the economic cost of providing loans at interest rates below market and represents management's estimate of the present value of projected net cash flows to the City from the loan portfolio.
- Estimated valuation of property held for resale was based on the most recently available consultant analysis of estimated values performed at the request of a creditor and sales prices previously received from recent solicitations that resulted in purchase and sale agreements.
- Estimated liabilities for workers' compensation claims were based on management's estimate obtained from information derived from Intercare's (a third-party administrator) claims database system adjusted for a discounted projection of unreported claims at 2.0%. Estimated liabilities for general liability and other claims were determined by the City Attorney's judgment about the ultimate outcome of the claims.
- Useful lives for depreciable property were determined by management based on the nature of the capital asset. Depreciation was calculated based on the straight-line method.
- Accrual of compensated absences was based on accrued eligible hours of vacation, sick leave and other compensatory time at current pay rates for eligible employees.
- Pension plans' employer and employee contributions requirements, net pension liability, and related deferred outflows and inflows of resources were based on actuarial valuations.
- OPEB plans' employer and employee contributions requirements, net OPEB liability, and related deferred outflows and inflows of resources were based on actuarial valuations.

- Accrual and disclosures of pollution remediation obligations were determined by the City's Environmental Compliance Officers and its environmental consultants' judgments about the ultimate outcome of the obligations.

Except for the fair value of the Pension Trust Funds investments and the pension and OPEB plans information based on actuarial valuations, we evaluated the key factors and assumptions used to develop these accounting estimates in determining that they are reasonable in relation to the financial statements taken as a whole. The fair value of the Pension Trust Funds investments and the pension and OPEB plans information based on actuarial valuations was agreed to the separately audited financial statements of the Pension Trust Funds, which were reported on by other auditors. Certain financial statement disclosures are particularly sensitive because of their significance to financial statement users. The most sensitive disclosures affecting the financial statements were as follows:

- The City's Defined Benefit Retirement Plans and Postemployment Benefit Plans Other than Pension Plans described in Note IV.A.
- Disclosures regarding the Successor Agency to the Redevelopment Agency of the City of San José described in Note IV.C.

The financial statement disclosures are neutral, consistent and clear.

Difficulties Encountered in Performing the Audit

We encountered no difficulties in dealing with management in performing and completing our audits.

Corrected and Uncorrected Misstatements

Professional standards require us to accumulate all known and likely misstatements identified during the audit, other than those that are trivial, and communicate them to the appropriate level of management. The attached is Schedule of Uncorrected Misstatements, which summarizes the uncorrected misstatements identified during our audit of the City's financial statements. Management has determined that their effects are immaterial, both individually and in the aggregate, to the financial statements as a whole.

During the audit, claims liabilities in the amount of $6,791,155 were accrued in the San José Clean Energy enterprise fund as a result of applying audit procedures and were subsequently corrected by management.

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 that no such disagreements arose during the course of our audit.

Management Representations

We have requested certain representations from management that are included in the management representation letter dated November 14, 2019.

Management Consultation with Other Independent Accountants

In some cases, management may decide to consult with other accountants about auditing and accounting matters, similar to obtaining a "second opinion" on certain situations. 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 statements, our professional standards require the consulting accountant to check with us to determine that the consultant has all the relevant facts. To our knowledge, there were no such consultations with other accountants.

Other Audit Findings or Issues

We generally discuss a variety of matters, including the application of accounting principles and auditing standards, with management each year prior to retention as the City's auditors. However, these discussions occurred in the normal course of our professional relationship and our responses were not a condition to our retention.

II. Other Matters

We applied certain limited procedures to the management's discussion and analysis; the schedules of revenues, expenditures, and changes in fund balance – budget and actual for the General Fund, Housing Activities Fund, and Low and Moderate Income Housing Asset Fund; the schedule of employer contributions – defined benefit pension plans; the schedule of changes in the employer's net pension liability and related ratios for the measurement periods ended June 30 – defined benefit pension plans; the schedule of investment returns – defined benefit pension plans; the schedule of the City's proportionate share of the net pension liability and related ratios – CalPERS; the schedule of employer contributions - CalPERS; the schedule of changes in the employer's net OPEB liability and related ratios for the measurement periods ended June 30 – postemployment healthcare plans; the schedule of employer contributions – postemployment healthcare plans; and the schedule of investment returns – postemployment healthcare plans, which are required supplementary information (RSI) that supplement the basic financial statements. Our procedures and the other auditors procedures for the Pension Trust Funds consisted of inquiries of management regarding the methods of preparing the information and comparing the information for consistency with management's responses to our inquiries, the basic financial statements, the separately audited financial statements of the Pension Trust Funds, and other knowledge we obtained during our audit of the basic financial statements. We did not audit the RSI and do not express an opinion or provide any assurance on the RSI.

We were engaged to report on combining and individual fund financial statements and schedules listed as supplemental information, which accompany the financial statements but are not RSI. With respect to this supplementary information, except for the supplementary information for the Pension Trust Funds, we made certain inquiries of management and evaluated the form, content, and methods of preparing the information to determine that the information complies with accounting principles generally accepted in the United States of America, the method of preparing it has not changed from the prior period, and the information is appropriate and complete in relation to our audit of the financial statements. We compared and reconciled the supplementary information to the underlying accounting records used to prepare the financial statements or to the financial statements themselves. The supplementary information for the Pension Trust Funds was agreed to the separately audited financial statements of the Pension Trust Funds, which were reported on by other auditors.

We were not engaged to report on the introductory and the statistical sections, which accompany the financial statements but are not RSI. We did not audit or perform other procedures on this other information and we do not express an opinion or provide any assurance on it.

SCHEDULE OF FINDINGS AND MANAGEMENT RESPONSES

Finding 2019-001 – Material Weakness
Internal Controls Over the Financial Reporting Process

The San José Clean Energy enterprise fund (the Fund) accounts for the City's Community Choice Energy program, which is a new program that began operations during the current fiscal year. This is a locally controlled electricity generation service provider to residents and businesses within the City of San José. This program allows the City to procure electricity for the residents and businesses of the City with more renewable energy options.

As part of our audit procedures, we review a letter from the City Attorney's Office that summarizes potential losses of the City. During our review of this letter, we discovered that a fine was imposed on the City by the State's Public Utility Commission in the amount of $6,791,155. While the City is appealing the fine, the ultimate outcome of the fine is not yet determined. Under generally accepted accounting principles, the City should recognize a liability for losses that it considers probable. While the actual amount of the loss is not yet known, an estimated loss should be recorded in the financial statements to ensure the financial statements properly reflect this contingency. However, the City had not recorded a provision for this potential loss. Subsequently, the City recorded a claims liability in the amount of $6,791,155 to reflect this potential loss as of June 30, 2019. The City took a conservative position and recorded the full amount of the fine imposed, even though the City continues to negotiate a lower amount.

As discussed above, the Fund began operations during the current year and, accordingly, is initiating many new processes to manage this activity, which inherently increases the risk of material misstatement. As with any new process, an evaluation of key internal controls should be made to reduce these risks. Based on the omission of a liability that is material to the Fund, we observed a deficiency in internal control that is considered a material weakness.

We recommend that the City establish a process to identify and record contingent liabilities in the Fund, including a process that incorporates a dialogue between management of the Fund and other departments, such as Finance and the City Attorney's Office, to ensure the proper identification and estimation of contingent liabilities.

Management response

The Community Energy Department along with Management recognize the need to immediately strengthen and build the accounting function for the San Jose Clean Energy Program. Limited resources within the Department and lack of accounting expertise contributed to this error. As an immediate solution to the matter, a temporary senior accountant position will be added to the Community Energy Department. Additionally, the Finance Department will work with Community Energy Department to develop a financing plan for financial accounting and reporting for this enterprise for review and consideration during the FY 2020-21 budget process. The Finance Department will continue to provide oversight and assistance to the Department as new staff is hired and trained. Finally, the Finance Department will work with the City Attorney's Office prior to the end of each fiscal year to review potential losses and ensure they are appropriately accounted for in the City's financial management system prior to the end of each fiscal year.

Target Completion Date: June 30, 2020

Finding 2019-002 – Significant Deficiency
Completeness of the Schedule of Expenditures of Federal Award

Criteria
Title 2 - Grants and Agreements, Subtitle A - Office of Management and Budget Guidance for Grants and Agreements, Chapter II - Office of Management and Budget Guidance, Part 200 - Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards - Subpart F - Audit Requirements - Sec. 200.510 Financial Statements requires that the City prepare a schedule showing total expenditures for the year for each federal program.

Condition
The City's draft schedule of expenditures of federal awards (SEFA) included federal expenditures that fluctuated through the course of the audit for the Federal Emergency Management Agency's Disaster Grants - Public Assistance grant. The changes included the offsetting of expenditures reimbursed by insurance proceeds and adding additional expenditures identified during the closing of the books. The impact of these changes resulted in significant changes in federal expenditures during the audit process. The Disaster Grants – Public Assistance grant is managed by the City's Department of Parks, Recreation and Neighborhood Services.

The identification of major federal programs is largely based upon the federal expenditures incurred during the year and whether those federal expenditures (1) meet certain "Type A or Type B" thresholds and (2) are high risk due to the complexities of the program. Because the federal expenditures were fluctuating during the audit, we were unable to determine the ultimate number of major federal programs required to be tested until the SEFA was completed. The results of the major federal program determination identified an additional program required to be tested as major, which will delay the completion of the Single Audit for the current year.

Cause
The Disaster Grants – Public Assistance grant is a complex grant. The City incurred costs during major storms in 2017, which caused flooding, which it later applied for grant funding. Upon approval, the funding sources for disaster recovery included federal, state, and insurance proceeds These costs must be carefully captured and allocated among the individual funding sources. The Department of Parks, Recreation and Neighborhood Services did not properly capture, allocate, carefully review, and submit the federal expenditures to the City's Finance Department for inclusion in the SEFA.

Effect or Potential Effect
The City's SEFA serves as the basis for reporting federal expenditures to the federal grantor agencies and is used in determining the number of major programs required to be audited in a given fiscal year under the Uniform Guidance. Inaccuracies have the potential of affecting the programs selected for testing as major programs.

Recommendation
The City should continue to improve its process for reviewing federal expenditures reported in the SEFA by requiring management of each department to review and submit a detailed listing of expenditures, including the funding sources or local matching requirements, prior to being submitted to the Finance Department for inclusion in the SEFA. In addition, the Finance Department should analyze and reconcile the detailed listing of expenditures to the SEFA for each significant federal program prior to the City submitting such detailed listing to its external auditors.

Management response

This deficiency is not related to a program deficiency nor does it constitute a violation of the federally funded grant covenants. This finding is specifically related to internal control over financial reporting, and not related to federal awards compliance funding.

The FY 2019-20 Adopted Budget includes funding for two additional accountants and ongoing funding for accounting staff training in the Finance Department. The Finance Department recently recruited and hired two new accountants. After the onboarding and training of these new positions, the Finance Department will reallocate resources to have Senior Accountants and other management accountant positions to work with departments to ensure sufficient training, monitoring and outreach efforts are undertaken. Included in this training and outreach efforts will be focus on ensuring appropriate staffing levels (number and type) are assigned to grant program accounting in the departments.

While the City has improved its process for reviewing expenditures reported in the SEFA, there is room for continued improvement to ensure the accuracy of reporting the expenditures of Federal Awards, the City will update the federal grant guidance document and continue to work towards implementing the following steps to address this issue:

1. Departments will perform analytical review procedures (i.e. current year vs. prior year expenditure changes) of their grant inventory listings on a quarterly and annual basis for accuracy.
2. Departments will reconcile the federal expenditures reported on the grant inventory listing to amounts recorded in the City's Financial Management System (FMS). The Accounting Division staff will perform a detail review of reconciliation for each significant federal programs prior to their submission to the Auditors.
3. The Accounting Division will also provide training to its professional accounting staff in reviewing the grant inventory listing for reasonableness and perform analytical and due diligence procedures.

Target Completion Date: June 30, 2020

STATUS OF PRIOR YEAR'S FINDINGS

Finding 2018-001 – Significant Deficiency
Risk Assessment of Internal Controls Over the Financial Reporting Process

Between 2006 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. Between 2015 and 2017, the City started to address its staffing challenges by filling vacant positions and adding three new personnel in the Finance Department. While the City has been successful in recruiting professionals to fill vacant positions over the past two years, it has been challenged with retaining these professionals. As such, the City has been continuously training and integrating new personnel into the City's complex accounting and financial reporting process. This rebuilding of staff has increased the workload of the remaining seasoned professionals.

The City has started to make investments in improving its financial reporting process over the past years; however, progress has been hampered by turnover of its recent hires. We recommend that the City evaluate the reasons for the increase in turnover and develop a plan to retain its personnel. In addition, the City should continue to incorporate the skills and experience of its new personnel assigned to key roles in the preparation of the annual financial statements to improve the efficiency of its financial reporting process, including cross-training to minimize the impacts of further turnover.

Status: Corrected.

Finding 2018-002 – Significant Deficiency
Completeness of the Schedule of Expenditures of Federal Award

During our audit, we noted the City's draft schedule of expenditures of federal awards (SEFA) included the Highway Planning and Construction (HPC) Cluster expenditures that were overstated by $9,439,739 due to management oversight. Management included expenditures other than the federal portion in its grant inventory listing. The Highway Planning and Construction Cluster is managed by the City's Departments of Transportation, Planning, Building and Code Enforcement, and Parks, Recreation and Neighborhood Services.

These errors resulted in additional major programs for the fiscal year 2018 as the type A and type B threshold decreased. The City subsequently corrected the expenditures reported in its fiscal year 2018 SEFA.

The City should continue to improve its process for reviewing expenditures reported in the SEFA by requiring department management to review and submit a detail listing of expenditures prior to being submitted to the Finance Department. In addition, the Finance Department should reconcile the detailed listing of expenditures to the SEFA for each significant federal program prior to the City submitting such detailed listing to its external auditors.

Status: Partially Corrected. While the City has improved its process for reviewing expenditures reported in the SEFA, we did identify a SEFA related finding in the current year (i.e. Finding 2019-002).

Finding 2018-003 – Significant Deficiency
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 previous audit 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. Prior year auditor 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
	Baseline security configuration setting and
Acceptable use	monitoring
Access to network and systems	Auditable event and monitoring
	Application change & emergency change
Anti-virus	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 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.

Status
Corrected. Management finalized its formal policies and procedures related to IT control processes. In addition, periodic scanning report and monitoring alerts, and tenable scanner was put in place to monitor and perform security configuration management via vulnerability scanning and recommended settings per software vendor.

Finding 2018-004 – Significant Deficiency
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 Privilege 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.
e. *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 a system / tool was utilized to make direct changes to production data for a system tested. This tool enables users to bypass transactions made via the applications in the normal course of business, circumvent manual controls in place and update data directly in the database. Per discussion with Management, users require approvals before making changes to data via this tool; however; there were no systematic restrictions that required approvals prior to the updates being made.

Shared Accounts

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

Audit Logging and Monitoring

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

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.

<u>Password Configuration</u>

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

Corrected. Management finalized its formal policies and procedures related to IT control processes. This includes password policy and privileged user management procedures.

Finding 2018-005 – Significant Deficiency
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.

Status
Corrected. Change control board/activity documentation implemented.

CITY OF SAN JOSE
Report to Those Charged With Governance
For the Year Ended June 30, 2019

SCHEDULE OF UNCORRECTED FINANCIAL STATEMENT MISSTATEMENTS

PJE#		Account / Adjustment Description	Debit (Dollars in thousands)	Credit
1	San Jose Financing Authority	Interest Payable	$ 358	$ -
	San Jose Financing Authority	Interest Expense	-	358
		(To adjust the interest payable accrued for 2001 Series A - 4th & San Fernando).		
2	Airport	Deferred outflows of resources	2,202	-
	Airport	Deferred inflows of resources	-	2,202
	Wastewater Treatment System	Deferred outflows of resources	5,925	-
	Wastewater Treatment System	Deferred inflows of resources	-	5,925
	Municipal Water System	Deferred outflows of resources	676	-
	Municipal Water System	Deferred inflows of resources	-	676
	Parking System	Deferred outflows of resources	240	-
	Parking System	Deferred inflows of resources	-	240
	Governmental Activities	Deferred inflows of resources	9,043	-
	Governmental Activities	Deferred outflows of resources	-	9,043
		(To increase deferred outflows and inflows of resources for pension related items, as changes to the total pension liabilities should be reported in separate categories instead of being netted together. This entry will not be recorded in the financial statements as the impact of netting balances together is not significant).		