CITY OF SAN JOSÉ

Report to Those Charged with Governance

For the Year Ended
June 30, 2017

CITY OF SAN JOSÉ

City Council For the Year Ended June 30, 2017

Table of Contents

Management and City Council
City of San José, California

Grant Thornton LLP
10 Almaden Boulevard, Suite 800
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 José, California (collectively, the "City"), as of and for the year then ended June 30, 2017, 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 José ("SARA"), the Norman Y. Mineta San José International Airport, the Police and Fire Department Retirement Plan, the Federated City Employees' Retirement System, the San José –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, 2017.

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 May 2017.

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 including Governmental Activities and Business-Type Activities, 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.

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 items represent particularly sensitive accounting estimates - allowance for receivables, 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.

Regarding the allowance for loan losses, another particularly sensitive accounting estimate, while we are satisfied regarding the presentation of management's estimate in the context of the financial statements taken as a whole as a result of other audit procedures applied during the engagement, we do not believe management has a reasonable basis for its estimate, as further discussed below in "Disagreements with Management" and "Material Weaknesses."

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. As outlined below, we reported a material weakness in internal control related to the lack of evidence supporting incurred losses on loans receivable and the resulting loan loss reserve reported in the Housing Activities Fund and the Low and Moderate Income Housing Asset Fund. Management believes its process for estimating incurred losses complies with US GAAP as outlined by the Government Accounting Standards Board (GASB) and we disagree. Consistent with the fundamentals outlined in GASB Statements 34 and 62, we believe losses and reserves should be recorded when underlying transactions (loss events) occur within the loan portfolio. These loss events are not tracked by the City, thereby bypassing the very data which would provide evidence of collectability and the measurement of losses. Further, the City is unable to otherwise support the assumptions used in its reserve process to produce its estimate of the allowance for loan losses.

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 José, California (the "City") as of June 30, 2017 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.

Material weaknesses

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. 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 City's financial statements will not be prevented, or detected and corrected, on a timely basis.

Our consideration of internal control was not designed to identify all deficiencies in internal control that, individually or in combination, might be material weaknesses; therefore, material weaknesses may exist that were not identified. However, we consider the following identified control deficiency to be a material weakness.

Finding 2017-001 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 $ 135 million and $ 509 million, respectively, at June 30, 2017. Of those loan balances, management recorded an allowance for uncollectible loans for 47% and 55%, respectively, of the gross loan balances in these two governmental funds which are maintained on the modified accrual basis of accounting. In addition to these reserves on loan principal, management also reserved 100% or $128 million of accrued

interest on these loans as uncollectable at the government-wide level which is presented on the a full accrual basis of accounting. Management's estimates for the governmental funds were made using a methodology combining an allowance for collectability risk and an allowance for present value discount at 1%. Management's methodology is documented and has been consistently applied for several years but the assumptions were not supported by evidence of incurred losses on loans such as historical results, industry data, and actual performance of individual loans or current credit quality of the borrower. Many of these traditional measures of loan losses were not tracked by the City and, therefore, were not factored into the loan loss calculation.

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

> An estimated loss from a loss contingency (as defined in paragraph 96) should be accrued if both of the following conditions are met:
>
> (a) Information available prior to issuance of the financial statements indicates that it is probable that an asset ***had been impaired*** or a liability ***had been incurred at the date of the financial statements***. It is implicit in this condition that it should be probable that one or more future events will occur confirming the fact of the loss.
> (b) The amount of the loss can be reasonably estimated.

Management was asked to provide evidence supporting the reasonableness of assumptions applied in the estimate of uncollectible loans. For example, we inquired about the policy to record a 40% reserve on certain categories of loans. While management was able to share an 11-year old point system which has evolved to a blanket 40% reserve, neither that evolved point system nor the resulting 40% had any relationship to incurred loan losses on these loan portfolios. Therefore, management was not ultimately able to adequately support the assumptions applied even though they were able to demonstrate they had complied with their policy.

With respect to the 1% discount factor, a factor which represents 27% of the recorded reserves, management has characterized this as an opportunity cost discount in its loan loss policy (lost earnings by virtue of the monies being invested in loans instead of an investment portfolio). This same 1% was characterized differently in the footnotes to the financial statements as an adjustment for below-market interest rates. Management was unable to explain how their 1% discount aligned with US GAAP but did relay on several occasions that they "make the market" on their loans and their actual interest rates of 0-6% and loan terms were market; not below market. In management's response below, however, management indicates "When this type of loan is made to developers and low income residents, the fair value of the loan receivable becomes less than its face value. In other words, this type of affordable housing loan receivable cannot be sold at its face value in the market."

In this regard, we find the City's documentation and explanations about market vs. below-market interest rates and loan terms to conflict with one another and the concept of opportunity cost appears to have no support in US GAAP.

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

Finally, management has shared with us discussions they've had with several other cities in California who have housing loans along with a State housing department. These other agencies have different loan loss reserve levels ranging from 0-100% of the loan balance. Management has interpreted this variety to be evidence of a widely recognized and prevalent industry standard in setting loan reserves. We view the dissimilar reserve results to indicate other agencies simply have different results after applying their policies. No evidence of a recognized and prevalent industry standard in establishing loan reserves was provided. Further, management has not articulated how the methodologies of each of these other agencies are used or their applicability to the City's particular loan portfolio. The City's assertion has, essentially, been that they can set the reserve by policy which is inconsistent with US GAAP.

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

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

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

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

Management response (unaudited)

Summary of Management's Response
Management had multiple discussions with Grant Thornton explaining and clarifying the affordable housing loan program and what the City is trying to measure with respect to the loan reserves. Management had explained to Grant Thornton why the current methodology for loan loss reserve is acceptable under GASB rules. The City has used this methodology for twenty-eight years and while this methodology may be "old

model" it has withstood internal and regular audits. In addition, City staff had inquired with other cities in California and verified that there is a wide range of reserve rates used by other local governments, and the practice of estimating reserves based on each entity's analysis of their unique affordable housing loan programs in their communities is widely recognized and prevalent within local governments. Accordingly, to conclude that the City's loan reserve measurement does not align with US GAAP, would conclude that many governments are not in compliance with US GAAP.

Management disagrees with Grant Thornton that an incurred loss model (described in second paragraph under "Condition") must be used when estimating loan loss reserves. The incurred loss model is not specified in GASB Statements 34 or 62. The incurred loss model is a topic in FASB ASC 450, Contingencies. GASB 34 states "revenues, expenses, gains, losses, assets, and liabilities resulting from exchange and exchange-like transactions should be recognized when the exchange takes place". Grant Thornton is interpreting this as equivalent to the incurred loss model described in FASB ASC topic 450. We disagree. GASB 62 states "an estimated loss from a loss contingency should be accrued if information available prior to issuance of the financial statements indicates that it is probable that an asset had been impaired at the date of the financial statements, and the amount of loss can be reasonably estimated". From an accounting perspective, an asset is impaired when its fair value is less than its book value. Unlike traditional mortgage loans, most of the City's affordable housing loans do not have fixed repayment schedules, requires payments due only in years when the projects report earning positive cash flow, and can be renegotiated to extend loan terms for continuing affordable housing purposes. When this type of loan is made to developers and low income residents, the fair value of the loan receivable becomes less than its face value. In other words, this type of affordable housing loan receivable cannot be sold at its face value in the market. Therefore, a loan loss reserve is established when an affordable housing loan is made.

As GASB does not have any statement addressing the method for estimating affordable housing loan loss reserves, GASB 76 allows a government to use practices that are widely recognized and prevalent in state and local government. The City's point system provides a fair and consistent way of estimating loan loss reserves. Reserves are based on loan type (e.g. construction, permanent), project type (e.g. multi-family, shelter, special needs), City's loan position (first, second, third, fourth), other lender/regulatory requirements, loan performance, strength of developer, and other unique issues to the project. Loan risks are reviewed annually for relevance. The City tracks actual loan loss event and accounts for it promptly: when an actual loss event occurs, the City writes off the loan receivable and related loan loss reserve.

The City's disagreement with Grant Thornton on this issue does not warrant a material weakness comment from Grant Thornton on the City's internal control as the City views its methodology to be consistent with GASB 76. The City has worked diligently to provide the documentation and reasoning behind its methodology; demonstrated its relevance; and inquired with its peer agencies, and the Government Finance Officers Association (GFOA), and Government Accounting Standards Board (GASB) regarding the appropriateness of its estimates. Furthermore, for the second year in a row, Grant Thornton was able to independently develop an estimate within an acceptable range of the recorded balance to satisfy its audit objective. This indicates that the risk of a material misstatement is remote.

Management's Response

The City's loan loss reserve is conservatively estimated to address the essence of the housing loan program – affordability and the loan loss reserve allowance is management's estimate of potential credit losses in the

affordable housing loan portfolio. The City's loan loss reserve ensures that the City recognizes in its financial statements that these loans were made to ensure affordability for our extremely low, very low, low, and moderate income residents. Loan repayments depend on the negotiated structure of the deal. The City's developer loans are not typically structured like traditional mortgages with fixed payment terms. Instead, many of the loans are structured to have payments due only in years when the projects report earning positive cash flow, or "residual receipts". Some are focused so heavily on extremely low income and/or special need populations that they expect no positive cash flow during the entire affordability restriction period. As such, the City's loan loss reserve recognizes the possibility that some of these loans likely will not be fully repaid and/or may be renegotiated to extend affordability for our lowest income residents.

The City believes that the methodology for loan loss reserve is acceptable under GASB rules. The City has used this methodology for twenty-eight years and this methodology has withstood internal and regular external audits. The City's methodology includes a risk evaluation model and assigns points to various loan criteria: loan type, project type, City's loan position, other lender/regulatory requirements. Under the current methodology, project loans and individual borrower loans that make scheduled payments during a fiscal year are evaluated for both discount and risk factors. Other project loans and individual borrower loans are grouped together by loan type, payment type or other common factors for the purpose of calculating a global discount and risk factor on the aggregate total of the group.

Loans are secured by first, second, third or lower in lien-property deeds of trust except for first time homebuyer loans, which are all secured by second deeds of trust. Interest and principal are typically due in installments, except for first time homebuyer loans, which do not require payments until their maturity dates.

The City has also invested in multi-family rental housing projects serving extremely low to moderate income individuals through subordinate loans with terms of up to 55 years. Generally, these loans are to be repaid through fixed payments or net cash flow payments from project operations and the term and potential risk of each loan varies. Because of the net cash flow feature of these subordinate loans, there is greater risk of variability in the timing of payments and, potentially, a lower probability of eventual repayment on these subordinate loans than on other loan types.

The City maintains a valuation allowance against loans receivable comprised of an allowance for risk and an allowance for present value discount. The allowance for risk is maintained to provide for losses that can be reasonably anticipated. The allowance is based upon continuing consideration of changes in the character of the portfolio, evaluation of current economic conditions, and such other factors that, in the City's judgment, deserve recognition in estimating potential loan losses. The allowance for risk takes into consideration maturity dates, interest rates, and other relevant factors.

In accordance with City policy, loans are funded at below market rates of interest and include amortized net cash flow deferred repayment terms. This policy exists to enhance the well-being of the recipients or beneficiaries of the financial assistance, who, as described above, are very low, low, or moderate-income individuals or families, or developers of housing for such individuals or families.

Accordingly, for financial statement purposes, the City has established an allowance account against the loans receivable balance containing a present value discount. The present value discount gives recognition to the economic cost of providing loans at interest rates below market, and represents an estimate of the present value of projected net cash flows to the City from the loan portfolio. The present value discount attributable to the loans will be recognized as interest income only as such loans are repaid in full because of the deferred nature of the loan portfolio and the high level of uncertainty relating to the likelihood that cash flows will occur as projected. The difference between the individual outstanding loan balances and the calculated net present value of the loans results in the allowance for present value discount. Losses are recognized as an addition to the allowance and any subsequent recoveries are deducted from the allowance.

Grant Thornton reported the same comment last year as significant deficiency because the City was unable to provide evidence to support the assumptions for estimating the loan loss reserve. The City, including the Housing Department, has experienced high personnel turnover in the last five years resulting in misplaced documentation. In August 2017, the City located the evidence supporting the assumptions applied in the estimate under the City's current methodology. In addition to providing the evidence, the City performed and provided additional analyses to demonstrate the relevance of the current methodology to the Housing loan portfolio. The City also inquired with peer agencies and had reached out to GFOA and GASB, both organizations stated that if the City has compelling evidence that the methodology is prevalent in the government industry and the City has applied that methodology on a consistent basis, the City does follow the requirements of USGAAP.

Management disagrees with Grant Thornton in its comment that the City's current methodology for estimating loan loss reserve is not consistent with the requirements of US GAAP. The City as governmental agency, is required to follow GASB Standards for accounting and financial reporting practices. The incurred loss model recommended by Grant Thornton, which is described in FASB ASC topic 450, Contingencies, is not specified in GASB statements. Pursuant to GASB Statement 76, if the accounting treatment for a transaction is not specified in GASB Statements, GASB Technical Bulletins, GASB Implementation Guides, and literature of the AICPA cleared by the GASB, a government entity can apply sources of nonauthoritative accounting literatures, such as FASB statements or practices that are widely recognized and prevalent in state and local government or others. No other government agency that the City inquired with uses incurred loss model in estimating their housing loan loss reserves and Grant Thornton was unable to provide a city or government agency that they audited that uses the incurred loss model that they recommend. Thus the City is hesitant to depart from GASB guidelines and move to incurred loss model for estimating loan loss reserves.

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 2017-002 Untimely identification of errors and lack of or inaccuracies in account reconciliations

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

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

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

We noticed several areas where this challenge was apparent:

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

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

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

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

Management response (unaudited)
Management concurs that account reconciliations between the subsystem and the general ledger should be performed at a regular basis (at least annually).

Due to some reporting functionality issues arising from the implementation of a new billing software at the end of June 2015, City staff was unable to maintain its previous process of monthly reconciliations. City staff has reconciled account balances on an annual basis for the fiscal years 2015-16 and 2016-17. The revenue management team, within the Finance Department is currently working with the software vendor to generate proper reports with more robust visibility as to the details of the billing cycles required to reconcile efficiently, and is in the testing phase of reconciling batch controls of the subledger to the general ledger on a monthly basis. The monthly reconciliation between the subsystem and the general ledger will be fully operational before the end of the fiscal year 2017-18.

In regard to the transactions recorded in the Housing Activity Fund and the Low and Moderate Housing Fund, account reconciliations are performed on a monthly basis and loan balances are reconciled against the subsystem on a quarterly basis. Management in the Housing Department will review journal entries and account reconciliations to identify errors in a timely manner. In addition, the Housing Department is in the process of reviewing older loans to ensure the terms entered in the database are up to date.

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

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

(a) develops, documents, and disseminates to appropriate personnel, policies that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the policy and associated controls; and,

(b) periodically reviews and updates the current policy and procedures.

Condition

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

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

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

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

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

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

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

Cause

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

Effect or Potential Effect

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

Failure to perform network security vulnerabilities and penetration assessments increases the risk that the information system's security weaknesses are not identified and investigated in a timely fashion.

Failure to implement and monitor recommended security configuration and best practice settings increases the likelihood of misconfigurations that may be exploited.

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

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

Management Response (unaudited)

- The most focused area of effort for Management has been on PCI compliance. Since November 2016, the City completed security reviews through Verizon Enterprise Solutions and Trustwave in early 2017; worked across departments to complete documentation of access and controls; reviewed and updated access; and secured the network, data, and applications environment for almost all transactions governed by PCI requirements. A small number of documentation items are still due from departments and Parking-related processes will be covered under a new vendor and contract currently in procurement.
- Management created and funded a Cybersecurity Office and City Information Security Officer (CISO) position as part of the 2017-2018 City Budget. Responsibilities for information and systems security are now designated as a responsibility of the group and the City is in the process of staffing. Progress in some areas of security have been limited by staffing limits.

- The new Information and Systems Security Policy remains in draft pending the hiring of the CISO. Edits were made to the draft to include feedback from the Grant-Thornton audit, City Auditor's audit of General Controls, and to match the policy to the National Institute of Standards and Technology Cybersecurity Framework. Management has completion of the new policy associated with the on-boarding of the new CISO, allowing the individual to apply their expertise, help guide the policy through to approval, and then create the City's educational content based on it.
- BitSight conducted a high-level scan of systems, behaviors, diligence, and breaches as indicators for the City to focus efforts.
- Management, through the IT Department, completed a draft of a Cybersecurity Assessments and Advanced Services Request for Proposals (RFP) to cover monitoring, security assessments/audits, education and tracking, incident response, and Virtual Security Operations Center services in October. Staff will review the RFP with the Purchasing Division for publication by January 2018 and award by the end of fiscal year 2017-18.
- Recognizing the increased risks associated with the City's decentralized information and systems control environment, the new CISO will have Citywide authority. Further, the CISO will work with designees for specialized security requirements affecting decentralized information and systems, such as PCI-DSS, CJIS, and HIPAA. These designees will serve as Component Security Officers (CSO) managing least-permissive rights and periodic reviews for financial, public safety, and human resources systems.

Finding 2017-004 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

Account Management

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

Password Configuration

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

Broad / Privileged User Accounts

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

Shared Accounts

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

Audit Logging and Monitoring

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

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

Management Response (unaudited)

- Management, through the IT Department, addressed future Account Management through implementation and usage of GroupID, which allows for the ability to synchronize IT Roles-based Access Control (RBAC), authentication profiles, and related settings from the City's Human Resources Management Systems. New employee accounts are created and managed through a single process, initiated by the Human Resources Department. Work remains on reviewing and cleaning existing application accounts, as well as on legacy network accounts that have been managed by decentral IT staffs to date.
- Password controls are addressed in the draft Information and Systems Security Policy. Password policy settings—expiration, complexity, et al— have already been implemented and are being enforced through the City's Active Directory group policies. Work remains and will be a focus for the new cybersecurity staff, once hired.
- Broad/Privileged User Accounts have been audited. Shared accounts have not been audited, but are not an approved practice as of July 2017. Significant work remains and these items will be a focus area for the new cybersecurity staff, once hired.
- Audit Logging and Monitoring remain basic and ad hoc. The activity is included on the City's Cybersecurity Workplan, to be handled through the Cybersecurity Assessments and Advanced Services Request for Proposals (RFP), once awarded. Currently, logging for central IT systems is occurring through SolarWinds Log and Event manager, a basic SIEM tool. Practices still need to be improved for alerting or filtering. Because of the speed at which cybersecurity threats and TTPs are evolving, the IT Department plans on utilizing vSOC services for this function if it's financially feasible.

Finding 2017-005 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 (unaudited)

- Management, through the IT Department, has a standardized Change Management process, including recent addition of system security review. IT staff is progressing beyond upgrades and updates, which are currently conducted, to include:
    - Formal approval processes with stakeholders;
    - More in-depth security reviews;
    - Use of standard access form with periodic auditing;
    - Documenting all changes and auditing against the change log; and
    - Broadening the Chance Management Board to include more stakeholders.

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

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

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

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

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

Effect or Potential Effect
Adjustments to leveling classification.

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

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

Office of Retirement Services Response (unaudited)
Within the Office of Retirement Services, the Accounting division coordinated with the Investments division to ensure that investment securities were categorized according to the proper level per GASB 72. The process was initiated by the Accounting division and reviewed for any changes for the current year by the Investments division. In the process of transferring the data from one worksheet to another by Accounting, two line items each consisting of a different fund manager, out of 743 line items rolling up to 75 fund managers, were inadvertently put in the wrong spot; thus causing the reclassification identified by the auditors. In the future, ORS will implement a final review by the Investments division to ensure their changes are captured.

Status of Prior Year Findings

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

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

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

The process of preparing an accurate CAFR is complicated by the variation in levels of supervisory review, reconciliation and processing flows within the finance and other departments along with the inconsistencies in accounting background among the departments. That coupled with employee turnover among finance functions and in the departments contributes to a challenge in maintaining an internal control environment to prepare an accurate CAFR.

We noticed several areas where this challenge was apparent:

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

Cause

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

Effect or Potential Effect

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

Status:

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

Finding 2016-002 Controls over estimating loan loss reserves

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

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

We recommend management review loan reserve methodology in the context of applicable accounting standards and enhance documentation supporting the basis for assumptions and rates applied to the loans to estimate the reserve. We were able to independently develop an estimate within an acceptable range of the recorded balance to satisfy our audit objective.

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

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

Status:
See Finding 2017-001.

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

Criteria

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

(a) develops, documents, and disseminates to appropriate personnel, policies that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the policy and associated controls; and,

(b) periodically reviews and updates the current policy and procedures.

Condition

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

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

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

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

Policies in draft	Not addressed in policy
Acceptable use	Baseline security configuration setting and monitoring
Access to network and systems	Auditable event and monitoring
Anti-virus	Application change & emergency change management

Business continuity and disaster recovery	Incident response
Data classification and handling	Vulnerability scanning
Encryption	Security training
Information security	Backup and data retention
Network security	
Password	
Secure system development	

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

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

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

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

Failure to perform network security vulnerabilities and penetration assessments increases the risk that the information system's security weaknesses are not identified and investigated in a timely fashion.

Failure to implement and monitor recommended security configuration and best practice settings increases the likelihood of misconfigurations that may be exploited.

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

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

Status:
See finding 2017-003.

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

Criteria

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

Account Management includes the following criteria:

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.

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

Condition

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

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

Account Management

- Management did not have a process to consistently document and retain approvals related to initial authorization and ongoing changes to user's access for seven systems tested.

- Management did not perform periodic access recertification for users (including privileged users) and system accounts for 11 systems tested.
- Management did not define the timeframe in which a separated employee or contractor's access from the Network must be disabled after separation and the timeframe in which a reassigned employee's access must be reviewed and updated after reassignment.

Password Configuration

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

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

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

Broad / Privileged User Accounts

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

Shared Accounts

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

Audit Logging and Monitoring

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

Cause

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

Effect or Potential Effect

Account Management

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

Password Configuration

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

Broad / Privileged User Accounts

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

Shared Accounts

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

Audit Logging and Monitoring

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

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

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

Finding 2016-005 Information Technology: Change Management

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

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

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

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

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

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

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

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

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

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

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

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

Status:
See Finding 2017-006

Finding 2016-007 Procurement under Federal Uniform Guidance

Federal Award: WIA/WIOA Cluster, CFDA 17.258, 17.259, 17.277, 17.278
Federal Award: Airport Improvement Program, CFDA 20.106

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

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

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

Questioned Costs
$0

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

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

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

Status:
Remediated

Finding 2016-008 Evaluating controls over third party service providers

Criteria
Management is responsible for the preparation and fair presentation of the financial statements in accordance with US GAAP. This includes the design, implementation, and maintenance of internal control relevant to the preparation of financial statements that are free from material misstatement, whether due to fraud or error. Effective internal controls include the monitoring of third party service providers who process transactions on behalf of the City.

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

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

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

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

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

Status:
Remediated

Finding 2016-009 Financial Reporting Controls

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

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

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

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

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

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

Status:
Remediated

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.

Very truly yours,

Grant Thornton LLP

November 30, 2017
San José, California

Summary of Recorded Misstatements

Current Year Recorded Adjustments

		Opinion Unit	Account Name	Debit	Credit
1	GT	Muni Water	Accounts Receivable		1,872,288
		Muni Water	Metered Recycled Water Sales	264,742	
		Muni Water	Metered Sales	1,520,117	
		Muni Water	Utility Tax Clearing	87,429	
		Purpose:To reconcile muniwater sub-ledger AR detail to GL at year-end			
2	GT	Opinion Unit	Account Name	Debit	Credit
		Integrated Waste Management	Garbage Receivable		3,998,452
		Integrated Waste Management	Special Assessment Receivable	4,354,829	
		Integrated Waste Management	Garbage Collection Fees		356,377
		Purpose: To reverse entry previously recocrded and subsequently rebook with entry 2.2 below for updated allocation.			
		Integrated Waste Management	Garbage Receivable		4,711,206
		Integrated Waste Management	Special Assessment Receivable	4,354,829	
		Integrated Waste Management	Garbage Collection Fees	356,377	
		Purpose:To correct original entry booked for the IMW receivable accrual when reconciling the sub-ledger AR detail to the GL			
3	GT	Opinion Unit	Account Name	Debit	Credit
		General Fund	Overpayment Holding Account	1,362,373	
		General Fund	Cash and Securities		1,362,373
		Integrated Waste Management	Cash and Securities	1,200,344	
		Integrated Waste Management	Garbage Receivable		1,200,344
		Muni Water	Cash and Securities	161,888	
		Muni Water	Accounts Receivable		161,888
		NonMajor Govt Funds	Cash and Securities	141	
		NonMajor Govt Funds	Accounts Receivable		141
		Purpose: To release overpayments of held as Other Liabilities to General fund to respective funds.			
4	GT	Opinion Unit	Account Name	Debit	Credit
		Integrated Waste Management	Garbage Receivable	590,319	
		Integrated Waste Management	Garbage Collection Fees		590,319
		Purpose: To adjust for differences between subledger detail provided and GL Balance.			

Summary of Unrecorded Misstatements

Current Year Passed Adjustments

GT	Opinion Unit	FS Line	Debit	Credit
	Muni Water	Revenues	424,325	
	Muni Water	Accounts Receivable		424,325
	Purpose: To adjust for differences between subledger detail provided and GL Balance.			

GT	Opinion Unit	FS Line	Debit	Credit
	Integrated Waste Manageme	Other Liabilities		1,684,138
	Integrated Waste Manageme	Accounts Receivable	1,684,138	
	Purpose: To reclassify credits from AR Subledgers to Other Liabilities as they represent an accumulation of Over Payments and not receivables.			

GT	Opinion Unit	FS Line	Debit	Credit
	Muni Water	Other Liabilities		338,327
	Muni Water	Accounts Receivable	338,327	
	Purpose: To reclassify credits from AR Subledgers to Other Liabilities as they represent an accumulation of Over Payments and not receivables.			

CSJ	Opinion Unit	FS Line	Debit	Credit
	NonMajor Govt Funds	Accounts Receivable		138,015
	NonMajor Govt Funds	Cash and Securities	138,015.00	
	NonMajor Govt Funds	Revenues		21,412
	NonMajor Govt Funds	Cash and Securities	21,412.00	
	NonMajor Govt Funds	Revenues		11,546
	NonMajor Govt Funds	Cash and Securities	11,546.00	
	NonMajor Govt Funds	Revenues		19,906
	NonMajor Govt Funds	Cash and Securities	19,906.00	
	General Fund	Cash and Securities	16,424.00	
	General Fund	Revenues		16,424
	Purpose: To record payments received in FY16/17. Payments were recorded into FMS in FY17/18.			

CSJ	Opinion Unit	FS Line	Debit	Credit
	Govt Activities- FS Only	Deferred outflow of resources		228,000
	Govt Activities- FS Only	Expenses	228,000	
	Purpose: To true up the pension contribution made in FY16/17. The amount originally deferred was $275,668K. The amount shown on the retirement CAFR were $136,957K and $138,483 (Total $275,440K)			

CSJ	Opinion Unit	FS Line	Debit	Credit
	Govt Activities- FS Only	Expense	2,073,315	
	Govt Activities- FS Only	Fund balance		2,073,315
	Purpose: To account for sewer trash catcher projects recorded in CY that should have been recorded in prior fiscal years			

CSJ	Opinion Unit	FS Line	Debit	Credit
	Waste Water	Expense		318,112
	Waste Water	Capital assets	318,112	
	Purpose: To capitalize the retention fund accrual.			

GT	Opinion Unit	FS Line	Debit	Credit
	Low and Moderate Income H	Allow for Uncollectible Loans	447,150	
	Low and Moderate Income H	Loans Receivable		447,150
	Purpose: To reduce the gross receivable balance of a loan that matured prior to year end (loan was fully reserved for therefore only impacted gross presentation)			

GT	Opinion Unit	FS Line	Debit	Credit
	Housing	Revenue	1,539,596	
	Housing	Fund Balance		1,539,596
	Purpose: To reclass release of liability recorded as revenue in the current year to prior year, as related expenses were incurred in PY.			

GT	Opinion Unit	FS Line	Debit	Credit
	Special Assessments	Revenue	424,896	
	Special Assessments	Revenue	674,296	
	Special Assessments	Revenue	72,131	
	Special Assessments	Fund Balance		424,896
	Special Assessments	Fund Balance		674,296
	Special Assessments	Fund Balance		72,131
	Purpose: To reclass special assessment revenue attributed to May 2016 recorded in July 2017			

Fund	Opinion Unit	FS Line	Debit	Credit
	Low and Moderate Housing	Allow for Uncollectible Loans		1,150,467
	Low and Moderate Housing	Revenues	1,150,467	
	Purpose: To increase reserve related to a loan with forgiveness clause that was only reserved at 40%.			

Reversing Impact of Prior Year Passed Adjustments (which have a current year impact)

GT	Opinion Unit	FS Line	Debit	Credit
	Housing	Fund Balance	54,638	
	Housing	Revenues		(54,638)
	Purpose: To record revenue in FY17 that was incorrect recognized in FY16.			

GT	Opinion Unit	FS Line	Debit	Credit
	General Fund	Fund Balance	2,288,511	
	General Fund	Expenses		(2,288,511)
	Purpose: To reclass impact of expenses recorded in FY17 that was were recognized in FY16.			

GT	Opinion Unit	FS Line	Debit	Credit
	General Fund	Fund Balance		(174,270)
	General Fund	Revenues	174,270	
	Purpose: To reduce revenue recorded in FY17 that was should have been recognized in FY16.			

GT	Opinion Unit	FS Line	Debit	Credit
	Municipal Water	Revenues	138,121	
	Municipal Water	Fund Balance		(138,121)
	Purpose: To reduce revenue recorded in FY17 that was should have been recognized in FY16.			

GT	Opinion Unit	FS Line	Debit	Credit
	Airport	Fund Balance		(2,499,203)
	Airport	Revenues	2,499,203	
	Purpose: To reduce revenue recorded in FY17 that was should have been recognized in FY16.