CITY OF
PALO
ALTO

POLICY AND SERVICES COMMITTEE

Tuesday, October 12, 2021
Regular Meeting
Virtual
7:00 PM

*****BY VIRTUAL TELECONFERENCE ONLY*****

Click to Join **Zoom Meeting ID: 946-1874-4621** **Phone: 1(669)900-6833**

Pursuant to the provisions of California Governor's Executive Order N-29-20, issued on March 17, 2020, to prevent the spread of Covid-19, this meeting will be held by virtual teleconference only, with no physical location. The meeting will be broadcast on Midpen Media Center at https://midpenmedia.org. Members of the public who wish to participate by computer or phone can find the instructions at the end of this agenda. Members of the public may speak to agendized items; up to three minutes per speaker, to be determined by the presiding officer. All requests to speak will be taken until 5 minutes after the staff's presentation. Public comment may be addressed to the full Policy and Services Committee via email at City.Council@cityofpaloalto.org and available for inspection on the City's website. Please clearly indicate which agenda item you are referencing in your email subject line.

Call to Order

Oral Communications

Members of the public may speak to any item NOT on the agenda.

Action Items

Presentation for all Items

1. Review and Approve a Task Order for the Office of the City Auditor to Conduct the Utility Work Order Process and Accounting Review

2. Office of the City Auditor Presentation of the IT Risk Management Assessment Report

3. Review and Approval of the Office of the City Auditor (OCA) Annual Report

Future Meetings and Agendas

Adjournment

PUBLIC COMMENT INSTRUCTIONS

Members of the Public may provide public comments to virtual meetings via email, teleconference, or by phone.

1. **Written public comments** may be submitted by email to city.council@cityofpaloalto.org.

2. **Spoken public comments using a computer or smart phone** will be accepted through the teleconference meeting. To address the Council, click on the link below to access a Zoom-based meeting. Please read the following instructions carefully.
    - You may download the Zoom client or connect to the meeting in- browser. If using your browser, make sure you are using a current, up-to-date browser: Chrome 30+, Firefox 27+, Microsoft Edge 12+, Safari 7+. Certain functionality may be disabled in older browsers including Internet Explorer. Or download the Zoom application onto your phone from the Apple App Store or Google Play Store and enter the Meeting ID below
    - You may be asked to enter an email address and name. We request that you identify yourself by name as this will be visible online and will be used to notify you that it is your turn to speak.
    - When you wish to speak on an Agenda Item, click on “raise hand.” The Clerk will activate and unmute speakers in turn. Speakers will be notified shortly before they are called to speak.
    - When called, please limit your remarks to the time limit allotted.
    - A timer will be shown on the computer to help keep track of your comments.

3. **Spoken public comments using a phone** use the telephone number listed below. When you wish to speak on an agenda item hit *9 on your phone so we know that you wish to speak. You will be asked to provide your first and last name before addressing the Council. You will be advised how long you have to speak. When called please limit your remarks to the agenda item and time limit allotted.

Click to Join **Zoom Meeting ID: 946-1874-4621 Phone: 1(669)900-6833**

AMERICANS WITH DISABILITY ACT (ADA)

Persons with disabilities who require auxiliary aids or services in using City facilities, services or programs or who would like information on the City’s compliance with the Americans with Disabilities Act (ADA) of 1990, may contact (650) 329-2550 (Voice) 48 hours or more in advance.

City of Palo Alto (ID # 13606)

Policy and Services Committee Staff Report

Report Type: Action Items **Meeting Date: 10/12/2021**

Title: Review and Approve a Task Order for the Office of the City Auditor to Conduct the Utility Work Order Process and Accounting Review

From: City Manager

Lead Department: City Auditor

The City Auditor recommends that the Policy & Services Committee approve the Office of the City Auditor's Utility Work Order Process & Accounting Review Task Order and recommend City Council for approval.

Discussion
In accordance with Baker Tilly's agreement with the City, the Office of the City Auditor is required to conduct activities each year. Those recurring activities include the execution of audits defined in the Audit Plan Presented to and Approved by P&S on February 9, 2021 and subsequently Presented to and Approved by City Council on March 1, 2021.

The Office of the City Auditor is seeking approval from the Policy & Services Committee of a Task Order to conduct the Utility Work Order Process & Accounting Review. Preliminary audit objectives include:

- Perform an initial assessment to identify high risk subprocesses in the work order process (e.g., labor, materials, specific utility).
- Document and evaluate the processes and controls in place to ensure proper recording of costs.
- Perform tests to determine the accuracy of attributed costs for a sample of completed work orders.

If approved unanimously by the Policy & Services Committee, this recommendation will be forwarded to the full City Council approval on an upcoming consent calendar.

Resource Impact
The budget for each Task Order noted above aligns to the previously approved budget for the Office of the City Auditor, the agreement with Baker Tilly, and the approved Audit Plan. Thus, there is no additional resource impact associated with this item.

Environmental Impact

Environmental review is not applicable to this activity.

Attachments:

- Task Order 11 - FY22 - Work Order Accounting & Process

Task Order 4.11 – Utility Work Order & Process Review

PROFESSIONAL SERVICES TASK ORDER

TASK ORDER 4.11 – FY22

Consultant shall perform the Services detailed below in accordance with all the terms and conditions of the Agreement referenced in Item 1A below. All exhibits referenced in Item 8 below are incorporated into this Task Order by this reference. The Consultant shall furnish the necessary facilities, professional, technical and supporting personnel required by this Task Order as described below.

CONTRACT NO.
OR PURCHASE ORDER REQUISITION NO. (*AS APPLICABLE*)

1A. MASTER AGREEMENT NO. (*MAY BE SAME AS CONTRACT / P.O. NO. ABOVE*):
1B. TASK ORDER NO.: FY21-001
2. CONSULTANT NAME: Baker Tilly US, LLP
3. PERIOD OF PERFORMANCE: START: October 1, 2021 COMPLETION: March 31, 2022
4 TOTAL TASK ORDER PRICE: $84,900
BALANCE REMAINING IN MASTER AGREEMENT/CONTRACT: Remaining in Task 4 FY22: $600,000
5. BUDGET CODE_______________
COST CENTER________________
COST ELEMENT______________
WBS/CIP__________
PHASE__________
6. CITY PROJECT MANAGER'S NAME & DEPARTMENT:
Lydia Kou, Chair of the City Council's Policy and Services Committee
7. DESCRIPTION OF SCOPE OF SERVICES (Attachment A)
MUST INCLUDE:
- SERVICES AND DELIVERABLES TO BE PROVIDED
- SCHEDULE OF PERFORMANCE
- MAXIMUM COMPENSATION AMOUNT AND RATE SCHEDULE (*as applicable*)
- REIMBURSABLE EXPENSES, if any (with "not to exceed" amount)

8. ATTACHMENTS: A: Task Order Scope of Services B (if any): N/A

I hereby authorize the performance of the work described in this Task Order.

APPROVED:
CITY OF PALO ALTO

BY:_________________________________
Name _______________________________
Title________________________________
Date ________________________________

I hereby acknowledge receipt and acceptance of this Task Order and warrant that I have authority to sign on behalf of Consultant.

APPROVED:
COMPANY NAME: ______________________

BY:_________________________________
Name _______________________________
Title________________________________
Date ________________________________

Attachment A
DESCRIPTION OF SCOPE OF SERVICES

Introduction

Attachment A, the Description of Scope of Services, contains the following four (4) elements:

- Services and Deliverables To Be Provided
- Schedule of Performance
- Maximum Compensation Amount and Rate Schedule (*As Applicable*)
- Reimbursable Expenses, if any (With "Not To Exceed" Amount)

Services & Deliverables

Baker Tilly's approach to conducting the Work Order Process Review involves three (3) primary steps:

- Step 1: Audit Planning
- Step 2: Process and Control Review
- Step 3: Reporting

Step 1 – Audit Planning

This step consists of the tasks performed to adequately plan the work necessary to address the overall audit objective and to solidify mutual understanding of the audit scope, objectives, audit process, and timing between stakeholders and auditors. Tasks include:

- Gather information to understand the environment under review
    - Understand the organizational structure and objectives
    - Review the City code, regulations, and other standards and expectations
    - Review prior audit results, as applicable
    - Review additional documentation and conduct interviews as necessary
- Assess the audit risk
- Write an audit planning memo and audit program
    - Refine audit objectives and scope
    - Identify the audit procedures to be performed and the evidence to be obtained and examined
- Announce the initiation of the audit and conduct kick-off meeting with key stakeholders
    - Discuss audit objectives, scope, audit process, timing, resources, and expectations
    - Discuss documentation and interview requests for the audit

Step 2 – Process and Control Review

This step involves executing the procedures in the audit program to gather information, interview individuals, and analyze the data and information to obtain sufficient evidence to address the audit objectives. The preliminary audit objective is to: (1) Determine whether adequate controls are in place and working effectively around the work order process; (2) Assess the work order process against best practices. Procedures include:

- Interview the appropriate individuals to understand the process, the information system used, and internal controls related to the work order process
- Review policies and procedures as well as the regulations and standards to identify the criteria to be used for evaluation of control design and effectiveness
- Perform a test of key internal controls on a sample basis
- Compare the process and controls against the best practices

Step 3 – Reporting

In Step 3, the project team will perform tasks necessary to finalize audit working papers, prepare and review a draft report with the stakeholders, and submit a final audit report. Tasks include:

- Develop findings, conclusions, and recommendations based on the supporting evidence gathered
- Validate findings with the appropriate individuals and discuss the root cause of the identified findings
- Complete supervisory review of working papers and a draft audit report
- Distribute a draft audit report and conduct a closing meeting with key stakeholders
    - Discuss the audit results, finings, conclusions, and recommendations
    - Discuss management responses
- Obtain written management responses and finalize a report
- Review report with members of City Council and/or the appropriate Council Committee
- Present the final report to the City Council and/or appropriate Council Committee

Deliverables:

The following deliverables will be prepared as part of this engagement:

- Audit Report

Schedule of Performance

Anticipated Start Date: October 1, 2021
Anticipated End Date: December 31, 2022

Attachment: Task Order 11 - FY22 - Work Order Accounting & Process (13606 : Approval of a Task Order to Conduct the Work Order Process

Maximum Compensation Amount and Rate Schedule

The not-to-exceed maximum, inclusive of reimbursable expenses (as summarized below) for this Task is $81,400. The not-to-exceed budget is based on an estimate of 400 total project hours.

Reimbursable Expenses

If circumstances allow, Baker Tilly anticipates planning one on-site fieldwork week. Given this possibility, Baker Tilly could incur reimbursable expenses for this Task.

The not-to-exceed maximum for reimbursable expenses for this Task is $3,500.

The following summarizes anticipated reimbursable expenses (for two team members):

- Round-trip Airfare – $1000
- Rental Car - $400
- Hotel accommodation - $1600 (4 nights)
- Food and incidentals – $500

Note that, if current restrictions associated with COVID-19 continue, an on-site visit may not be possible. The project team will work with the City to consider circumstances at the time.

City of Palo Alto

(ID # 13556)

Policy and Services Committee Staff Report

Report Type: **Meeting Date: 10/12/2021**

Title: Office of the City Auditor Presentation of the IT Risk Management Assessment Report

From: City Manager

Lead Department: City Auditor

Recommendation

The City Auditor recommends that the Policy & Services Committee consider the following actions:

1) Accept the IT Risk Management report and corresponding recommendations for improvement; and

2) Recommend the City Council approve the IT Risk Management Report

Executive Summary

Baker Tilly, in its capacity serving as the Office of the City Auditor, performed a review of Information Technology risk management practices as approved in the FY2021 Audit Plan approved by City Council.

Through the assessment activity, the Office of the City Auditor identified recommendations for improvement. The Information Technology Department is in general agreement with each finding and has drafted action plans for each item with some partial agreement in recognition of the necessity to scale the best practices to the size and scale of the City of Palo Alto and specifically to address current limited resources and prioritization of those resources. This, however, is taken into consideration in the management action plans developed by the Department.

The Office of City Auditor will perform periodic follow up procedures to validate that corrective actions have been implemented.

Background

The City's Information Technology Department provides technology services that support all City departments in delivering quality services to the community. To ensure that the City protects the value of its Information Technology Department and mitigates potential risks, Office of the City Auditor conducted an assessment of the Department's risk management practices. Key risks facing the Information Technology Department include cyber security, database/data management, and disaster preparedness and recovery risks.

The Office of the City Auditor included an assessment in the FY2021 Audit Plan approved by City Council. The objectives of this review were to:

1) Gain an understanding of the key risks areas within the City's IT governance strategy and the risk management environment.

2) Determine whether adequate controls are in place to ensure the security of information, and aligned with the City's strategic information technology goals.

Discussion

The attached report summarizes the analysis, audit findings, and recommendations.

Timeline, Resource Impact, Policy Implications

The timeline for implementation of corrective action plans is identified within the attached report. All corrective actions are scheduled to be implemented by FY 2023.

Stakeholder Engagement

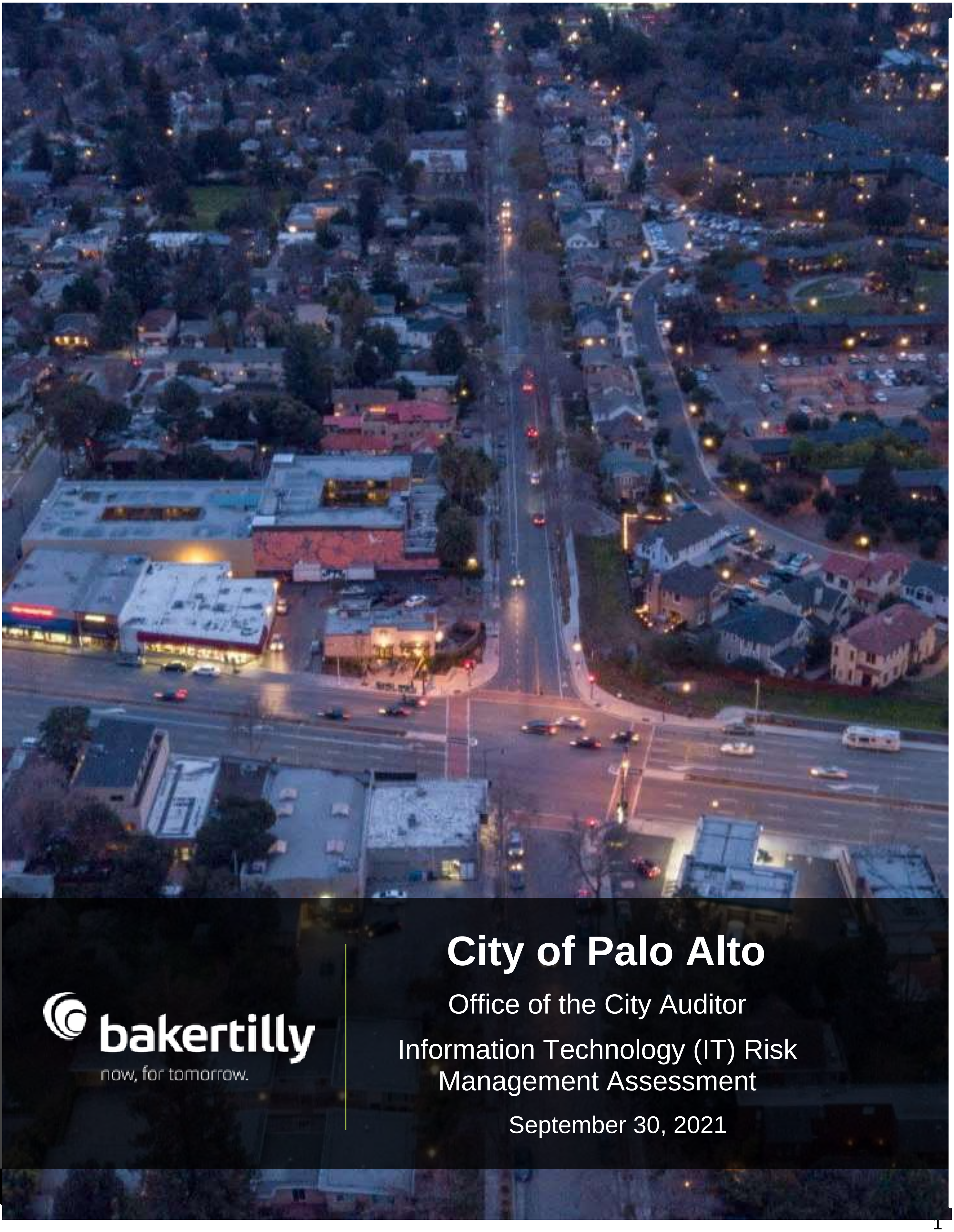
The Office of the City Auditor worked primarily with the Information Technology Department and engaged with additional stakeholders, including the City Manager's Office.

Environmental Review

Environmental review is not applicable to this activity.

Attachments:

- OCA - IT Risk Management - Final Draft (REDACTED)



City of Palo Alto

Office of the City Auditor

Information Technology (IT) Risk Management Assessment

September 30, 2021

bakertilly
now, for tomorrow.

Executive Summary

Purpose of the Audit

The purpose of this assessment was to gain an understanding of key risks areas within IT governance strategy and the risk management environment, evaluate the adequacy of the control environment and offer recommendations for improvement.

Report Highlights

Finding **Page 10**

Formalized IT Risk Management processes will further ensure the City's technology risks are properly identified, assessed, managed and monitored.

The City does not currently have formal IT risk management practices. In general, day-to-day operational controls are in place to mitigate IT risks, but gaps may still exist for unidentified IT risks, resources may not be prioritized to higher risk or strategically aligned areas, and senior management or oversight bodies may not receive timely awareness of risks affecting the City.

Key Recommendations to the City Manager:
The City should work to develop an overall IT risk management process that incorporates the following key steps:

- Setting Context for IT risk management including establishing a defined risk appetite, assigning employee responsibility and developing Key Performance Indicators (KPI) and metrics to evaluate the achievement of strategic objectives and outcomes.
- Establishing and conducting a formal Risk Identification and Assessment process including establishing techniques for risk identification with consideration for vulnerabilities, decomposing areas of concern and threats into statements of risk and maintaining a current risk register.
- Risk Analysis and Business Impact Evaluation beginning with adoption of a best-practice risk management framework and then developing a set of enterprise criteria to rank, rate, and assign disposition to accept, avoid, mitigate or transfer each risk.
- Identifying a Risk Response including assigning a risk disposition (i.e. response) to each risk, assigning responsibility for response, developing a risk mitigation and contingency plan, and performing periodic reevaluation of risk disposition as necessary.
- Conduct Risk Reporting and Communication including on-going monitoring of risk status, periodic reevaluation and progress reporting to all relevant stakeholders.

Page 31 In addition, the Information Technology Department should work to mitigate operational level risks, identified as part of this audit, on a prioritized basis as budget and resources allow.

Attachment: OCA - IT Risk Management - Final Draft (REDACTED) (13556 : Information Technology Risk Management Assessment Report)

Table of Contents

Executive Summary 2

Purpose of the Audit 2

Report Highlights 2

Introduction 4

Objective 4

Background 4

Scope 5

Compliance Statement 5

Detailed Analysis & Testing 6

Methodology 6

Approach 6

Assessment Results 7

Appendices 11

Appendix A: Risk Matrix 11

Appendix B: Risk Heat Map 25

Appendix C: Operational Level Risks and Considerations 28

Appendix D: Management Response 32

Introduction

Objective

The purpose of this assessment was to gain an understanding of key risks areas within IT governance strategy and the risk management environment, evaluate the adequacy of the control environment and offer recommendations for improvement.

Background

The City of Palo Alto's Information Technology Department exists "to provide innovative technology solutions that support City departments in delivering quality services to the community" according to their mission statement. These services support transportation, utilities, streets, fire, police and ambulance service provision. Disruptions in technology and unmitigated risks may prevent or delay residents from receiving vital services.

The City is a global technology hub and aims to reflect this in their city services. As Palo Alto aims to "build and enable a leading smart and digital city," there is a desire to adopt innovative technologies to improve residents' quality of life, serve commercial entities, and lead in sustainability. At the beginning of FY13, the Information Technology Department set a strategic direction to achieve these goals.

To ensure that the City protects the value of its Information Technology Department and mitigate potential risks, the City has decided to conduct an internal assessment of the Department. This decision was in conjunction with a broader, Citywide audit plan detailing the potential risks facing each department. The key risks facing the Information Technology Department include cyber security, database/data management, and disaster preparedness and recovery risks.

The Information Technology Department is governed by the municipal code, "section 2.08.240 Department of Information Technology", internal policies and procedures, and its operational divisions including the Office of the Chief Information Officer, the IT Project Management Office, IT Operations, IT Enterprise Services, and Information Security Services.

The City is also going through a number of large-scale initiatives, including a large upgrade to the City's Enterprise Resource Planning (ERP) system, implementation of a GIS system, and alignment of Data Strategy, Standardization, and Governance.

In 2020, Baker Tilly conducted an initial risk assessment, the City's current risk management control environment. As a result, the following findings were identified:

- There is no formal risk framework being followed.
- No risk register exists with identified risks and risk prioritization.
- No scoring or formal discussion of likelihood and severity or internal controls.
- Palo Alto does not have a comprehensive strategic IT Capital Plan.

In order to properly assess the City's IT risk management environment, we utilized COBIT 5 and Risk IT Management best practice frameworks, which were developed and published by the Information Systems Audit and Controls Association (ISACA). The frameworks offer a practical approach to evaluate risks associated with processes, organizational structures, culture, policies, information, infrastructure and people from a functional and management perspective. More details on these frameworks are included in the Detailed Report Approach and Methodology section.

Scope

We reviewed the City's IT governance, risk management, and operational level controls documentation for the period March 1, 2020 through February 28, 2021.

Compliance Statement

This audit activity was conducted from March 2021 to September 2021 in accordance with generally accepted government auditing standards, except for the requirement of an external peer review[1]. In addition, certain technical specialists do not adhere to the Continued Professional Education (CPE) requirements outlined in the generally accepted government auditing standards. A mitigating factor, however, is that the City Auditor oversees all work and does adhere to the CPE requirements.

Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The Office of the City Auditor greatly appreciates the support of the IT Department in conducting this assessment.

Thank you!

[1] Government auditing standards require an external peer review at least once every three (3) years. The last peer review of the Palo Alto Office of the City Auditor was conducted in 2017. The Palo Alto City Council approved a contract from October 2020 through June 2022 with Baker Tilly US, LLP (Baker Tilly) and appointed Kyle O'Rourke, Senior Consulting Manager in Baker Tilly's Public Sector practice, as City Auditor. Given the transition in the City Audit office, a peer review was not conducted in 2020 and will be conducted in the second year of Baker Tilly's contract.

Attachment: OCA - IT Risk Management - Final Draft (REDACTED) (13556 : Information Technology Risk Management Assessment Report)

Detailed Analysis & Testing

Methodology

Baker Tilly's objective is to evaluate the City's IT implementation of risk management processes. We noted that similar organizations adopt processes from a variety frameworks and elected to compare common criteria to evaluate the current state of risk management at the City of Palo Alto. Baker Tilly developed recommendations for the implementation of a risk management program using the framework, known as COBIT 5, which was developed and published by ISACA. This provided a baseline to evaluate the IT Department's mitigating control policies and procedures related to governance, IT risk management framework, IT risk management process, event identification, risk assessments, IT risk response and maintenance and monitoring of IT risk action plans. COBIT 5 is an umbrella framework which aligns with the standards below:

1. ISO 31000 (2009): Risk Management Principles and Enablers
2. ISO/IEC 27005 (2011): Information Security Risk Management
3. COSO ERM: Integrated Framework which includes the eight components of COSO Enterprise Risk Management (ERM)

Additionally, the Information Systems Audit and Controls Association (ISACA) *Risk IT Framework, 2nd Edition* and IT Risk Management Work Program, both aligned with COBIT and industry best practices, were referenced in assessing the City's IT risk management environment.

Approach

The following approach was performed for the IT risk management assessment:

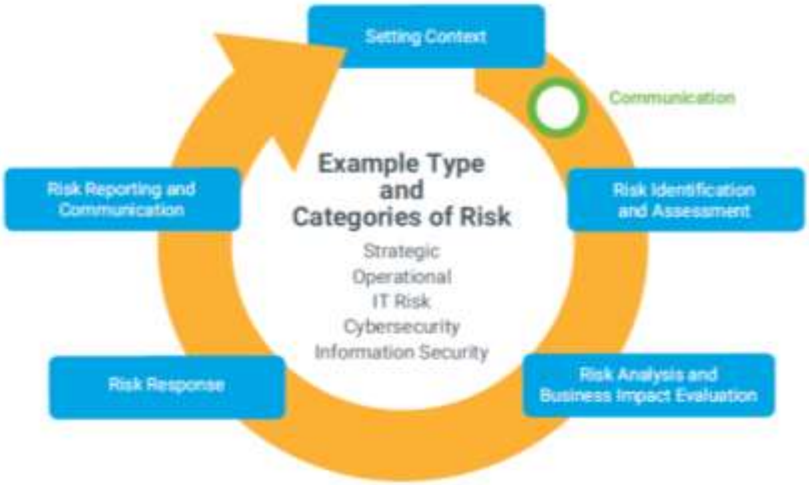
1. Request and review background information to obtain an understanding of the Risk Management and Governance strategy within the City of Palo Alto.
2. Conduct interviews with key process owners and management to gain understanding of the City's IT risk management strategy, risk assessment process, and any security baselines and frameworks
3. Assess risks and identify controls in place
4. Test design and implementation of controls related to assessment objectives to determine whether controls are adequately designed and implemented to support the IT Risk Management Strategy
5. Compare the current IT risk management process against appropriate IT governance and security frameworks
6. Document findings and validate with process owners
7. Draft report

Assessment Results

Finding 1 Formalized IT Risk Management processes will further ensure the City's technology risks are properly identified, assessed, managed and monitored.

Summary The City does not currently have formal IT risk management practices. In general, day-to-day operational controls are in place to mitigate IT risks, but gaps may still exist for unidentified IT risks, resources may not be prioritized to higher risk or strategically aligned areas, and senior management or oversight bodies may not receive timely awareness of risks affecting the City.

The key components of risk management as covered in the Risk Management Workflow from the *Risk IT Framework, 2nd Edition*, encompasses the five steps illustrated below:


Setting Context
Communication
Risk Identification and Assessment
Risk Analysis and Business Impact Evaluation
Risk Response
Risk Reporting and Communication
Example Type and Categories of Risk
Strategic
Operational
IT Risk
Cybersecurity
Information Security

Source: Adapted from ISACA, *Getting Started With Risk Management*, USA, 2018, fig. 2, *https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpgsr*

1. Setting Context: Understand risk to the City in the context of its mission, strategy, and objectives and identify resources required to deliver the services that align with the City's priorities.
2. Risk Identification and Assessment: Establish a register of all any internal and external IT risks that will impact the City's ability to achieve its objectives.
3. Risk Analysis and Business Impact Evaluation: Use standard criteria to measure the likelihood, impact, frequency and magnitude of the risk scenarios from a top-down or bottom-up approach.

4. Risk Response: Based on the analysis and the organization risk appetite, plan and implement a mitigation approach to avoid, share, transfer or accept the risks.
5. Risk Reporting and Communication: Monitor risks and report timely and accurate risk information to decision makers and stakeholders (including oversight bodies).

We are presenting our findings and recommendations for the City below as it relates to each of these five steps of the Risk Management Workflow.

Step 1: Setting Context includes establishing a risk appetite, communication of risk vision, employee responsibility and identifying high-value services and products to support critical asset risk management. Understanding the threats to the City's strategic plan is essential to ensuring risk management controls add value to the risk management process. Failure to define the City's threat landscape may result the inability to protect against and respond in the instance where an event occurs. Disruptions in technology and unmitigated risks may prevent or delay residents from receiving vital services.

We reviewed the Palo Alto IT Strategy FY19-FY21 and found that critical assets have been identified, prioritized and the strategy has been communicated to employees. However, employee responsibilities and action plans have not been identified, a risk appetite has not been established and Key Performance Indicators (KPI) and metrics to evaluate the achievement of strategic objectives and outcomes of the plan were not developed.

We recommend The City establish its risk appetite and tolerance when developing strategy. Implementing a proactive IT risk management process is critical because the IT Departments provides numerous technology needs Citywide for Palo Alto. The strategy should be communicated to all stakeholders to ensure there is an understanding of their respective risk management roles and responsibilities. Critical assets should be identified and prioritized to determine what services and products are necessary for service delivery. An effective IT strategy can bring many benefits to an organization, including lower costs, greater control, more efficient and effective use of resources, and overall better strategic alignment and risk management.

Step 2: Risk Identification and Assessment includes establishing techniques for risk identification with consideration for vulnerabilities, decompose areas of concern and threats into statements of risk and compare to current risk register. Preemptively, assessing the loss-event scenarios that can impact the entire City is a proactive approach that is essential during the risk management process. Failure to identify historical, present and emerging risks may result in reduced confidence or visibility into any risks that can impede the City's ability to meet its objectives.

The City does have operational level controls and processes to identify specific vulnerabilities. However, the City does not have an overall formal risk identification process, risk register or risk assessment process. Due to the lack of risk register, Baker Tilly conducted numerous interviews with key IT staff and end-users in each IT functional area to gain insight into the IT environment. The purpose of the interviews was to gain a general understanding of the controls in place to mitigate the associated risks within each IT area. Through these interview discussions and review of documentation we developed the IT Risk Matrix in Appendix A and identified opportunities for the City to further improve upon and reduce risk within IT operations. Information on the specific risk observations are included in Appendix C.

Attachment: OCA - IT Risk Management - Final Draft (REDACTED) (13556 : Information Technology Risk Management Assessment Report)

We recommend The City develop a criteria to identify risk. Inputs include an inventory of the vulnerabilities, processes, assets, and groups of people in an organization so that consideration can be given to potential for adverse impacts. Risk identification and categorization can occur through many methods such as Strength, weakness, opportunity and threat (SWOT) analyses, Business impact analyses (BIA), Scenario analysis and Risk and control self-assessments (RCSA). Each method provides an opportunity to consider potential events that may prevent the achievement of business objectives. Then decompose the areas of concerns into a statement of risk and capture the conditions or situation that causes the concern, and an impact statement that describes the outcome of the realized risk. After these exercises, the register can be continuously compared against the risk statements on an on-going basis.

Step 3: Risk Analysis and Business Impact Evaluation includes developing a set of enterprise criteria to rank and rate risk and assign disposition to accept, avoid, mitigate or transfer risk based on the related actions. An IT risk management best practice framework of choice should be leveraged as guidance when conducting a risk analysis to facilitate the establishment of a risk disposition. Failure to rank, rate and take a position on how to address risk may prevent the City's ability to respond to the most sensitive and critical events timely.

The City has not undertaken efforts for rating and ranking risks or conducting a business impact evaluation. A Citywide criteria has not been established based on an IT risk management framework. Important events and near misses around IT affecting the City are not identified, analyzed and risk-rated. Risk assessments are not performed on a recurrent basis, using qualitative and quantitative methods that assess the likelihood (probability) and impact of identified risk. As a result, Baker Tilly also assigned likelihood and impact ratings to each IT risk area within the Risk Matrix in Appendix A, and plotted them on a Risk Heat Map, included in Appendix B.

We recommend the City develop their own criteria for ranking the risks included in the risk analysis. The analysis should encompass first identifying threats to the City and then determining their likelihood, frequency and magnitude on the City. Then Citywide risk scenarios can be identified and analyzed. After analysis, the City can choose a risk disposition to address risk and the related scenarios based on the stated thresholds and/or events that are deemed unacceptable.

Step 4: Risk Response includes assigning a risk disposition (i.e. response), periodic reevaluation, assigning responsibility for response, and developing a risk mitigation and contingency plan. A disposition of accept, avoid, mitigate or transfer is usually assigned to each risk. Establishing actionable steps, assigning ownership and developing a formal risk response plan is critical to the risk management process. Failure to establish a process for responding to risk may result in the inability to mitigate risk timely due to a lack of resources and poor planning.

The City does have a security incident response process where ownership is assigned, response plan is identified/implemented with oversight, and incident records are documented and retained. However, overarching IT risk management response procedures have not yet been implemented. Additionally, risk action plans are not developed and therefore do not allow for proper monitoring to ensure implementation, identification of costs, benefits, responsibility and approval of remedial actions or acceptance of residual risk.

For proper risk response, management should internally review and select a disposition to address each risk. Per the Risk IT Framework, “Effective risk management requires mutual understanding between IT and the business regarding which risk needs to be managed and why.” An owner or responsible personnel should be identified for each risk and as conditions and the IT environment changes, the disposition should be revisited. A risk mitigation plan including mitigation activities, milestones and target completion date needs to be developed. Plan should also consider technology risk scenarios from a top-down or bottom-up approach, which both evaluate capabilities, timing, people, processes and physical infrastructure. Top-down begins with a high-level view of mission and strategy; whereas Bottom-up begins with critical assets, application or systems across the City. In the event internal mitigation is too costly, a contingency plan can be established to minimize the risk impact.

Step 5: Risk Reporting and Communication includes on-going monitoring of risk status, periodic reevaluation and progress reporting to all relevant stakeholders. Once an IT risk management plan is in place, it is important to continuously communicate the status to all involved stakeholders to ensure the plan is adequate to meet the needs of the current IT environment. The inability to communicate the current state of risks timely may prevent senior management from being able to respond appropriately. Additionally, a lack of engagement may produce incomplete or ineffective mitigation efforts due to excluding stakeholder feedback when revisiting, reassessing and updating the plan based on ever-changing Citywide internal and external risk factors.

Palo Alto does have periodic reporting to City Council related to budget and large Citywide projects. However, there is no formal process for IT Management and City Council's regular and routine consideration, monitoring and review of IT risk management.

We recommend Palo Alto establish a risk reporting structure. Risks should be identifiable, recognized, well understood and known and managed through application of appropriate resources. This ensures there is a common understating of the City's risk exposure and increases transparency into the threat defenses the City has at its disposal. Risk should be monitored and risk mitigation plans updated as conditions change, if needed.

To effectively report on risks, there should be a clear understanding and training, as needed, on the City's risk management strategy and any related policies and procedures. Any areas where the City's current capabilities are lacking should be communicated so that the necessary resources can be obtained to enhance the risk management process expeditiously. Once the risks have been identified, status reporting should include the risk profile, Key Risk Indicators (KRIs), event/data loss, a root cause analysis and migration options. Per the Risk IT Framework, "Information must be communicated at the right level of detail and adapted for the audience."

Appendices

Appendix A: Risk Matrix

IT Risk Area	Risk Factors	Current Controls and Practices	Likelihood	Impact	Rating
Application Management This area focuses on the management of the organization's business applications – how they are developed, procured, modified and managed as well as how application security is performed and the role of the IT department in managing an application. **Risk Statement** Poor application management practices causing application downtime or lack of functionality resulting in disruption of business operations.	• Lack of application integration • Inability to implement application changes and provide application support in a timely manner due to critical staff shortage or turn-over • Disruption of core business functions due to application downtime • Opportunity and/or revenue loss due to lack of application functionality • Increased risk of data breaches	**REDACTED**	**Low**	**Med**	**Med**

Attachment: OCA - IT Risk Management - Final Draft (REDACTED) (13556 : Information Technology Risk

Palo Alto IT Risk Management Assessment
Appendix A: Risk Matrix

IT Risk Area	Risk Factors	Current Controls and Practices	Likelihood	Impact	Rating
Architecture and Deployment This area focuses on the architecture and deployment of organization's information technology. In-scope elements include: • The network architecture and deployed technology that is used to provide intra-site, inter-site connectivity and Internet connectivity • The organization's server and storage infrastructure • The computer hardware that is deployed for end-users **Risk Statement** Poor IT architecture and deployment causing unreliable IT service delivery and security weaknesses resulting in end-user dissatisfaction or loss of data availability, integrity, or confidentiality and reputational damage.	• Poor or unreliable IT service delivery • End-user dissatisfaction • Security weaknesses	REDACTED	Low	Med	Med

Attachment: OCA - IT Risk Management - Final Draft (REDACTED) (13556 : Information Technology Risk

Palo Alto IT Risk Management Assessment
Appendix A: Risk Matrix

IT Risk Area	Risk Factors	Current Controls and Practices	Likelihood	Impact	Rating
Asset Management This area focuses on the IT department's asset management practices. In-scope activities include the following: • Tracking information technology assets from procurement through disposal. • Reusing and decommissioning information technology assets • Ensuring information technology assets have an assigned owner, who is a stakeholder in the asset's protection • Ensuring information technology assets are properly maintained to maximize their useful life • Tracking software usage and ensuring that vendors' software license agreements are followed **Risk Statement** Poor asset management practices resulting in loss of data and IT assets, decreased asset longevity and usefulness, increased costs due to unneeded asset acquisition, and increased security vulnerabilities for untracked IT assets.	• Inadequate security management of untracked IT assets • Lack of asset longevity and usefulness • Increased costs due to unneeded asset acquisition • Legal fines and reputational damage • Data loss	REDACTED	**Med**	**Med**	**Med**

IT Risk Area	Risk Factors	Current Controls and Practices	Likelihood	Impact	Rating
Change Management This area focuses on the IT department's practices for controlling changes to the IT environment. In-scope activities include the following: • Management of infrastructure hardware, software and configuration changes • Management of host system software and configuration changes • Management of normal and emergency changes • Application release management • Delineation of the activities that are controlled by change management versus help desk request ticketing **Risk Statement** Poor change management practices causing inappropriate, unauthorized, under-planned and/or under-tested system changes resulting in disruption to business operations.	• Inappropriate, unauthorized, under-planned and/or under-tested system changes may be implemented that negatively impact agency operations and/or reputation	REDACTED	**Low**	**Med**	**Med**
Compliance Management This area focuses on the IT department's practices for complying with IT-related contract requirements, governmental regulations (e.g., HIPAA Security Rule) and industry standards (e.g., PCI Data Security Standard). In-scope are the following activities: • Compliance program development and maintenance • Compliance program monitoring and reporting **Risk Statement** Insufficient compliance management practices causing non-compliance with requirements, laws or regulations resulting in penalties, fines, legal costs, and reputational damage.	• Regulatory fines and oversight stemming from non-compliance • Increased operating expenses (e.g., payment card transaction costs) • Legal costs and ramifications that damage reputation and hinder business operations	REDACTED	**Med**	**Med**	**Med**

Attachment: OCA - IT Risk Management - Final Draft (REDACTED) (13556 : Information Technology Risk

IT Risk Area	Risk Factors	Current Controls and Practices	Likelihood	Impact	Rating
Database and Data Management This area focuses on the IT department's practices for managing digital information. In-scope activities include the following: • Classifying the information that is received, processed, transmitted and stored by the work staff • Protecting digital information from the following security losses: confidentiality, integrity and availability • Controlling access to digital information via file share and database management controls • Performing procedures to backup stored information • Ensuring backed up information is recoverable **Risk Statement** Poor database and data management practices causing data loss and accidental or unauthorized data modification or disclosure resulting in unplanned staff time and expense to recover (reenter) lost data, disruption of business operations, and reputational damage.	• Accidental and unauthorized data modification or disclosure • Loss of data availability or usage • Unplanned staff time and expense to recover (reenter) lost data • Disruption of business processes and service delivery • Financial penalties for service level misses • Reputational harm	REDACTED	**Low**	**Med**	**Med**

IT Risk Area	Risk Factors	Current Controls and Practices	Likelihood	Impact	Rating
Disaster Recovery Preparedness and Testing This area focuses on the IT department's preparations and testing for disaster recovery (DR). In-scope activities include the following: • Disaster recovery strategy and alignment with the organization's business continuity plans • Disaster recovery plan preparation • Disaster recovery testing **Risk Statement** Insufficient disaster recovery preparedness causing less effective and timely recovery from disaster events, resulting in increased disruption of business operations and service delivery, expenditures for system recovery, and reputational damage.	• System and information unavailability • Disruption of business processes and service delivery • Financial penalties for service level misses • Unplanned expenditures for system recovery • Reputational harm	REDACTED	**Med**	**High**	**High**

IT Risk Area	Risk Factors	Current Controls and Practices	Likelihood	Impact	Rating
End-User Support and Perceptions This area focuses on the IT department's scope and approach for providing end-user support as well as the perceptions that end-users have regarding IT service delivery. In-scope activities include the following: • End-user request intake • Help Desk triaging of end-user requests and problems • Help Desk request tracking and reporting • End-user notification of request handling progress and completion • Requesting and receiving end-user feedback on completed or abandoned service requests **Risk Statement** Poor end-user support causing customer dissatisfaction resulting in loss of end-user sponsorship and partnership in IT initiatives, and loss of IT funding.	• Loss of IT funding • Loss of end-user sponsorship and partnership in IT initiatives	REDACTED	**Med**	**Low**	**Med**

IT Risk Area	Risk Factors	Current Controls and Practices	Likelihood	Impact	Rating
Host Intrusion and Malware Defense This area focuses on the IT department's practices for protecting network connected computers, telephones, printers and infrastructure hardware devices from intrusive activity and malicious software exploitation. In-scope activities include the following: • Intrusion detection and prevention deployment, operation, and monitoring • Malware defense deployment, operation (e.g., signature updating), and monitoring for hosts and applications (e.g., spam email) **Risk Statement** Poor host intrusion and malware defense practices resulting in system vulnerabilities/weaknesses that lead to a loss of data availability, integrity, or confidentiality, reputational damage, and/or monetary loss and penalties.	• Loss of system/application availability and integrity • Loss of data confidentiality, integrity and availability • Data breach and hijacking (ransomware) • Reputational damage • Monetary loss and penalties	REDACTED	**Med**	**High**	**High**

Attachment: OCA - IT Risk Management - Final Draft (REDACTED) (13556 : Information Technology Risk

IT Risk Area	Risk Factors	Current Controls and Practices	Likelihood	Impact	Rating
Information Security This area focuses on the IT department's practice of information security. Information security programs are developed to protect an organization's information systems and information from plausible threats and vulnerability exploitation that could result in one or more losses of security: confidentiality, integrity, availability, authenticity and/or non-repudiation. Programs should address the following: • Policy development and enforcement • Identity and access management • Threat identification and management • Vulnerability identification and management • Security roles and responsibilities • Security training and awareness for IT and non-IT personnel **Risk Statement** Under-developed information security program resulting in system vulnerabilities/weaknesses that lead to a loss of data availability, integrity, or confidentiality, reputational damage, and/or monetary loss and penalties.	• Inappropriate or unauthorized access (physical and logical). • Unclear responsibilities and performance requirements. • Increased probability that the systems and data within the systems are not adequately protected from technical and malicious threats.	REDACTED	**Low**	**High**	**Med**

IT Risk Area	Risk Factors	Current Controls and Practices	Likelihood	Impact	Rating
Mobile Device Management This area focuses on the IT department's management of mobile devices. In-scope activities include the following: • Authorization to use mobile devices • Mobile device provisioning, monitoring, support and deprovisioning • Mobile device incident response **Risk Statement** Poor mobile device management practices causing a data breach resulting in loss of data confidentiality.	• Unauthorized device access due to compromised security PINs • Installation of unwanted / malicious software on mobile devices • Non-detection of rooted (security compromised) mobile devices • Unauthorized access by installed mobile applications to stored email, text messages, media and data • Unauthorized user access to stored email, text messages, media and data as well as network applications via VPN • Loss of data confidentiality • Data breach • Reputational damage • Monetary loss and penalties	REDACTED	**High**	**Med**	**High**
Operations and Monitoring This area focuses on the IT department's practices for operating, monitoring and maintaining the computer systems and supporting infrastructure that are used by the work staff. In-scope activities include the following: • Capacity management • Hardware and software maintenance **Risk Statement** Poor computer operations and monitoring/maintenance practices causing loss of system security and availability, increased costs from insufficient planning/forecasting, and disruption of business operations.	• Loss of system security • Reduced system availability. • Increased costs due to insufficient planning and forecasting • Disruption of business processes and service delivery • Financial penalties for service level misses • Reputational harm	REDACTED	**Low**	**High**	**Med**

Attachment: OCA - IT Risk Management - Final Draft (REDACTED) (13556 : Information Technology Risk

Palo Alto IT Risk Management Assessment
Appendix A: Risk Matrix

IT Risk Area	Risk Factors	Current Controls and Practices	Likelihood	Impact	Rating
Organizational Architecture This area focuses on the organization of the IT department, its placement within the organization and its approach to staffing. **Risk Statement** Poor organizational structure and staffing causing communication gaps, lacking knowledge/skillsets, excessive workload, or decreased productivity resulting in poor service delivery.	• Lack of organizational structure and/or staffing to perform business-as-usual functions • Poor service delivery • Unfulfilled end-user and business sponsor expectations	REDACTED	**Low**	**Med**	**Med**
Physical and Environmental Controls This area focuses on IT physical and environmental safeguards that are deployed to protect the organization's application systems and information. In scope activities include the following: • Deployment and monitoring of physical access controls that protect IT assets • Deployment and monitoring of environmental controls that protect IT assets **Risk Statement** Lack of proper physical and environmental safeguards over data centers causing unauthorized access or physical damage resulting in loss of data or hardware.	• Inappropriate or unauthorized physical access to data centers, server rooms, wiring closets, or facilities containing end-user IT hardware • Inappropriate or unauthorized physical access to IT hardware • IT hardware and/or infrastructure loss due to poor environmental controls • Data loss or theft • System loss or theft • Data breach • Reputational damage • Monetary loss and penalties	REDACTED	**Low**	**High**	**Med**
Problem Management and Incident Response This area focuses on the IT department's practices for managing problems and incidents. In scope are the following activities: • The method(s) by which IT problems are reported and resolved• Problem tracking, reporting and communication • Incident response preparation and response testing	• Loss of IT asset confidentiality, integrity and availability • Physical loss and damage • Data breaches • Reputational damage • Monetary loss and penalties	REDACTED	**Med**	**High**	**High**

IT Risk Area	Risk Factors	Current Controls and Practices	Likelihood	Impact	Rating
- Incident identification, triaging, containment, eradication and recovery **Risk Statement** Ineffective management of IT problems and incidents causing loss of IT asset confidentiality, integrity and availability resulting in impacts to business operations, reputational damage, and/or monetary loss and penalties.					🟥
Procurement and Service Provider Management This area focuses on the IT department's practices for procuring hardware, soft-ware, facilities and services as well as managing the contracted service providers. In scope are the following activities: - Procurement strategy - Vendor and service provider due diligence and performance monitoring **Risk Statement** Insufficient procurement practices and oversight of vendors/service providers resulting in higher spending, product/service delivery problems, or security issues.	- Insufficient oversight of procurement strategy and methods could result in the failure to optimize the cost and effectiveness of IT asset and service purchases - Insufficient oversight of service provider contract performance could result in the non-timely detection of product/service delivery problems - Insufficient oversight of service provider activity and security controls could cause security problems including a data breach - Data breaches - Reputational damage - Monetary loss and penalties	REDACTED	**Med**	**Med**	**Med**

Palo Alto IT Risk Management Assessment
Appendix A: Risk Matrix

IT Risk Area	Risk Factors	Current Controls and Practices	Likelihood	Impact	Rating
Portfolio Project Management This area focuses on the IT department's project management practices. In-scope activities include: • Initiating, planning, executing, controlling, and closing projects • Managing projects' scope, milestones, quality and budget • Ensuring projects are adequately staffed • Reporting project progress and issues on a recurring basis to management and stakeholders **Risk Statement** Poor project management resulting in cost/schedule overruns or unmet customer needs, impacting business operations.	• Poor project deliverable quality • Project cost overruns • Late project completion • Unmet project stakeholder expectations • Fines due to unmet project milestones or non-compliance • Reputation harm	REDACTED	Low	Low	Low
Risk Management This area focuses on the IT department's risk management practices. In-scope activities include IT risk identification, triaging, treatment, tracking and management reporting. **Risk Statement** Lack of awareness and management of internal and external technology risks caused by inadequate risk management practices resulting in severe impacts to the City and its operations.	• Loss of IT asset confidentiality, integrity and availability • Physical IT asset loss and damage • Data breaches • Reputational damage • Monetary loss and penalties	REDACTED	Med	Med	Med

Appendix A: Risk Matrix

IT Risk Area	Risk Factors	Current Controls and Practices	Likelihood	Impact	Rating
Strategy and Governance This area focuses on IT strategy and governance practices. In-scope activities include the following: • Development, maintenance and approval of an IT strategic plan that is aligned with the organization's business strategy • Development and execution of tactical IT plans that are aligned to the IT strategy • Development, maintenance and approval of an IT operating budget • Recurring performance and risk reporting to Executive Management and the City Council • Oversight of IT operation and resource consumption by Executive Management and the City Council **Risk Statement** Poor IT strategy and governance practices resulting in the inability to properly oversee and manage IT functions and align with the City's needs and priorities.	• IT service delivery is misaligned with the organization • IT over-spends and under-delivers • Organizational needs and expectations with respect to information technology are not met • Executive management and the City Council are unaware of IT risks and their severity • All compliance and data-related risks previously listed	REDACTED	High	Med	High

Appendix B: Risk Heat Map

The risk heat map ranks the following IT risk categories plotted in the heat map based on risk scores. Related risk observations are also noted within (refer to Appendix C: Operational Level Risk Observations).

1. Mobile Device Management
2. Strategy and Governance
3. Disaster Recovery Preparedness and Testing
4. Host Intrusion and Malware Defense
5. Compliance Management
6. Database and Data Management
7. Problem Management and Incident Response
8. Risk Management
9. Asset Management
10. Compliance Management
11. Procurement and Service Provider Management
12. Information Security
13. Operations and Monitoring
14. Physical and Environmental Controls

RISK MAP			
	Low Impact	**Medium Impact**	**High Impact**
High Likelihood	**Risk Severity: Medium**	**Risk Severity: High** 1. Mobile Device Management: Observation 10 2. Strategy and Governance	**Risk Severity: Critical**
Medium Likelihood	**Risk Severity: Low** 1. End-User Support and Perceptions	**Risk Severity: Medium** 1. Asset Management: Observation 1, 2 2. Compliance Management: Observation 4, 5 3. Procurement and Service Provider Management: Observation 12, 13 4. Risk Management: Finding 1 - 5	**Risk Severity: High** 1. Disaster Recovery: Observation 7 2. Host Intrusion and Malware Defense 3. Problem Management
Low Likelihood	**Risk Severity: Negligible** 1. Portfolio Project Management: Observation 14	**Risk Severity: Low** 2. Application Management: Observation 3. Architecture and Deployment: Observation 4. Change Management: Observation 3 5. Database and Data Management: Observation 6 6. Organizational Architecture 7. Architecture and Deployment	**Risk Severity: Medium** 1. Information Security: Observation 8, 9 2. Operations and Monitoring 3. Physical and Environmental Controls: Observation 11

Risk Analysis Methodology

Baker Tilly used the Open Web Application Security Project's (OWASP) Risk Rating methodology generally across all IT areas, which assesses risk based upon the likelihood that a risk event will occur and its potential impact. The matrix shown in Table 1 considers technical likelihood and business impact to help determine the overall risk level.

Technical likelihood addresses the ease of identifying and exploiting the risk. This can be further understood by looking at "threat agents" and "vulnerability factors". Threat agents are the items that address the motive and skill required to exploit a risk. Vulnerability factors address the ease of identifying the risk and exploiting it.

Business impact addresses the exploitive effect of the vulnerability upon the business, consisting of "technical impacts" and "organizational impacts". The technical impacts are those that address the confidentiality, integrity and availability of the data. The organizational impacts are financial damage, reputational damage, regulatory non-compliance, loss of intellectual property and violation of privacy.

Table 1. Risk Rating

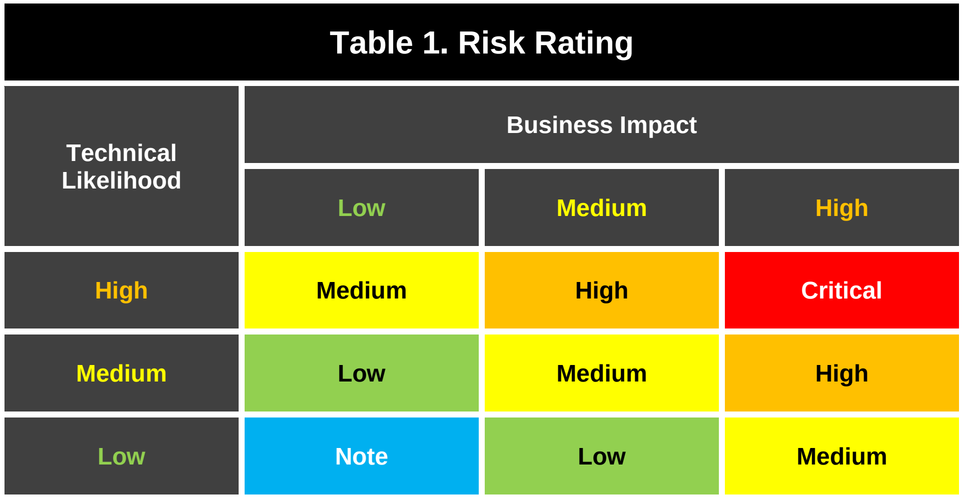


Table 1. Risk Rating

Technical Likelihood	Business Impact		
	Low	Medium	High
High	Medium	High	Critical
Medium	Low	Medium	High
Low	Note	Low	Medium

Each risk rating category has been described in Table 2 below.

Table 2. Risk Rating Category Descriptions

Table 2. Risk Rating Category Descriptions

Risk Rating	Description
Critical	These risks have both a high technical likelihood of occurrence and a high business impact upon the organization. Their exploitation could cause great damage to the organization, its systems and/or sensitive information assets. The underlying vulnerabilities should be treated as soon as possible.
High	These risks have mixed technical likelihood of occurrence and a business impact that ranges between medium and high. Their exploitation could cause much damage to the organization, its systems and/or sensitive information assets but the degree of damage is less than the critical risks. The underlying vulnerabilities should be treated with or after the “critical risk” vulnerabilities.
Medium	These risks have mixed technical likelihood of occurrence and a business impact that ranges between low and high. Their exploitation could cause moderate damage to the organization, its systems and/or sensitive information assets but the degree of damage is less than the high risks. The underlying vulnerabilities should be treated with or after the “high risk” vulnerabilities.
Low	These risks have mixed technical likelihood of occurrence and a business impact that ranges between low and medium. Their exploitation could cause nominal damage to the organization, its systems and/or sensitive information assets but the degree of damage is less than the medium risks. The underlying vulnerabilities should be treated with or after the “medium risk” vulnerabilities.
Note	These risks have both a low technical likelihood of occurrence and a low business impact upon the organization. Their exploitation would cause negligible damage to the organization, its systems and/or sensitive information assets but the degree of damage is less than the low risks. The underlying vulnerabilities may optionally be treated with or after the “low risk” vulnerabilities.

Appendix C: Operational Level Risks and Considerations

Opportunities exist to further improve upon and reduce risk within IT operations. While taking into consideration the risk levels associated with identified observations and focusing on areas with the highest impact and likelihood, we recommend that the Information Technology department work to mitigate identified risks on a prioritized basis, as budget and resources allow. *It is important to note that the IT risks observations included within this assessment are not all-inclusive of every possible threat that could impact the City. Rather, the scope is limited to risks identified during interview discussions and through review of documentation.*

IT Area	Risk/Observation and Recommendations
Asset Management	**Observation 1:** There is a lack of visibility when IT assets (systems, software, equipment/devices) are purchased with end user departmental budgets. This may contribute to decentralized shadow IT and the inefficient use of organizational resources by purchasing unnecessary software without IT's review and approval. **Recommendation 1:** We recommend that Palo Alto charter an Information Technology Committee to evaluate all IT system and application procurements and purchases for appropriateness to ensure risk management oversight, standardization and strategic alignment of IT investments, and prioritization of those most valuable and beneficial to the organization as a whole (driven by budget and resource availability).
	Observation 2: Asset tracking is manual in nature, monitored by multiple departments (i.e. Finance and IT) and there is an opportunity to increase the amount and type of information being captured. This may contribute to the inefficient and ineffective asset management. **Recommendation 2:** We recommend that Palo Alto procure an asset management tool to provide a more effective and centralized approach to manage assets, increase visibility into asset utilization, maximize asset life and reduce costs.
Change Management	**Observation 3:** Palo Alto does not have a change management policy. This may result in inconsistent and uncontrolled application and system changes. **Recommendation 3:** We recommend that Palo Alto formally document its change management process to ensure consistency with requests, testing, management approval and the implementation of changes to its applications and systems.
Compliance Management	**Observation 4:** There is no formal process to identify, document, and monitor compliance requirements. Lack of documented formal policies and procedures may result in unidentified compliance obligations and non-compliant business practices, which can lead to penalties, fines and an increased costs related employee training. **Recommendation 4:** We recommend that Palo Alto develop a compliance policy, which formally defines the City’s approach to compliance management. This will ensure employees are provided with guidance to perform their roles and responsibilities in an ethical manner that is in accordance with applicable laws and regulations and allow for a consistent, standardized process. **Observation 5:** Information Security Policy gaps and exceptions are documented in SharePoint through an Exception Form, and it was noted that Departments are allowed to request compliance exceptions without end dates. This may prolong the use of non-

Attachment: OCA - IT Risk Management - Final Draft (REDACTED) (13556 : Information Technology Risk

IT Area	Risk/Observation and Recommendations
	compliant business practices. Therefore, compliance related internal controls may be overridden which increases the City's risk exposure. **Recommendation 5:** We recommend that Palo Alto incorporate a requirement that exception duration dates must be provided on exception forms. For extenuating circumstances where a date cannot reasonably be determined, the requestor should be required to provide a remediation plan, which includes compensating controls to mitigate the risk exposure.
Database and Data Management	**Observation 6:** The City protects data that falls under key compliance areas such as PCI, HIPAA, CJIS and NERC/CIP. There is a draft Data Classification Policy, however, it has not been formalized and Citywide data has not been cataloged. This may result in the inability to protect unclassified data. Furthermore, lack of a formal policy which employees are required to acknowledge and adhere to may increase the risk of accidental and unauthorized data modification or disclosure. **Recommendation 6:** We recommend that Palo Alto finalize the Data Classification Policy, which should include the requirements for public, internal, confidential, restricted data and the impact of the data’s confidentiality, integrity and availability. Additionally, roles and responsibilities should be established related to data owners, data protectors, data users and include a rationalization for how data was classified.
Disaster Recovery Preparedness and Testing	**Observation 7:** The City does not have a formal disaster recovery plan. In 2014 a recovery plan was developed as a result of an audit, but it was not formalized. Lack of a tested recovery plan may result in the inability for the City to respond in the event of a disaster and the disruption of operations and resident services. **Recommendation 7:** We recommend that Palo Alto revisit the recovery plan previously developed. The plan should be updated based on the current IT environment and implemented Citywide. Development should incorporate a business impact analysis or related process to solicit information from the business units on recovery time objectives and recovery point objectives. The plan should include measures to address offline communication/building accessibility, software and hardware failures, downtime and data loss, designates roles during a disaster, the handling of sensitive information, cyberattacks and environmental catastrophes.
Information Security	**Observation 8:** The City has legacy and non-IT approved and procured applications that are not integrated with Active Directory (AD) and do not require network permissions to access City data. The City has taken the initiative to integrate single sign-on between Active Directory and all critical Citywide (enterprise) systems and applications but there are legacy systems and applications that have not been integrated. The lack of integration increases information/data risk exposure and the potential for applications that do not meet IT security standards and policy requirements. **Recommendation 8:** To ensure consistent adherence to security standards across the organization, we recommend the City continue to develop IT governance processes and standards to apply Citywide. It may also be prudent to reevaluate the non-AD integrated applications and systems housing non-critical data. The reevaluation will provide an opportunity to determine if there is any data still sensitive enough to be viewed as valuable to an attacker. In this case, said data and the respective applications and systems should be prioritized, as contracts and the budget allows, to integrate with AD.

Attachment: OCA - IT Risk Management - Final Draft (REDACTED) (13556 : Information Technology Risk

IT Area	Risk/Observation and Recommendations
	Observation 9: The City's legacy and/or shadow IT systems and applications are managed by each respective business unit. This may contribute to an inconsistent termination notification process and potentially prevent or delay the deprovisioning of user access depending on whom is managing the system or application. Additionally, Human Resources (HR), initiates the termination process in the SAP system, however, there can be a lag in notification from HR to the IT Department. This may result in IT receiving untimely notification of an employee separation to ensure that network access is disabled promptly. **Recommendation 9:** We recommend that Palo Alto develop a centralized termination notification process to ensure a consistent adherence to Citywide security standards. Designated systems and application owners should be identified and automatically notified when a termination occurs via the same automated ticketing process as IT personnel. The process should increase the communication of employee separations between Management and HR and then to the IT Department. Additionally, the specific access rights/privileges current users have to each system/application and should be reviewed for accuracy. This will reduce the risk exposure that terminated employees have unauthorized access.
Mobile Device Management	**Observation 10:** The City currently has an in-flight project to replace mobile devices that cannot be wiped. However, it has not been finalized. The inability to wipe mobile devices that have been, lost or stolen may result in the unintentional disclosure of confidential organizational data to a malicious attacker. **Recommendation 10:** We recommend that Palo Alto consider prioritization of the project to upgrade the devices, which will enhance security capabilities across all platforms and reduce Citywide risk exposure.
Physical and Environmental Controls	**Observation 11:** The Interim CIO manually requests a data center user access review for appropriateness from the Facilities Department on an ad hoc basis but the City does not perform formal user access reviews on at least an annual basis. In addition, we reviewed the data center access listing and noted 10 generic "Safety Keys" for the Fire Department, which are not assigned to a unique individual. These may result in unauthorized or inappropriate datacenter access. **Recommendation 11:** We recommend that Palo Alto Management conduct, document and retain data centers reviews on at least an annual basis to ensure users do not have access beyond their job responsibilities. Access should be designated to a unique employee based on role and need. In instances were generic "Safety Keys" are needed; they should be logged per user and monitored on a more frequent basis to ensure proper usage.
Procurement and Service Provider Management	**Observation 12:** Vendor contracts include a poor performance clause, which focuses on response time. However, vendor monitoring for quality, efficiency and effectiveness is not actively performed and expectations beyond response time are not established. Insufficient oversight of service provider contract performance could result in untimely detection of product/service delivery problems. **Recommendation 12:** We recommend that Palo Alto develop and incorporate service level agreements into City IT contracts. Agreements should include an overview, goals and objectives, stakeholders and periodic review requirements. Additionally, specifications should be included to cover the scope, customer requirements, service provider requirements, service assumptions and service management.

Attachment: OCA - IT Risk Management - Final Draft (REDACTED) (13556 : Information Technology Risk

IT Area	Risk/Observation and Recommendations
	Observation 13: Through discussions we noted the procurement process may cause delays in IT purchases and acquisitions. Delays in IT acquisitions may result in the disruptions of services to residents. **Recommendation 13:** We recommend that IT work with Purchasing, Legal and other stakeholders to identify ways to streamline IT procurement while maintaining procedural safeguards that protect the City. *Note: The City Auditor will also incorporate and consider IT purchase practices during the 2022 Risk Assessment process.*
Project Management	**Observation 14:** Palo Alto appears to have a knowledgeable and experienced project management group. However, the IT Playbook (project management guide) is outdated and not fully utilized as a resource by staff. Outdated policies and procedures may result in inconsistent project management, lack of knowledge retention and poor delivery which can cause end-user dissatisfaction. **Recommendation 14:** We recommend that Palo Alto Management review and update the Playbook once a year to ensure project management personnel have accurate information and resources to be able to perform their job responsibilities consistently and in accordance with standards and expectations.

Appendix D: Management Response

Recommendation	Responsible Department(s)	Agree, Partially Agree, or Do Not Agree and Target Date and Corrective Action Plan
Finding: Step 1 – Setting Context		
Setting Context includes establishing a risk appetite, communication of risk vision, employee responsibility and identifying high-value services and products to support critical asset risk management. Understanding the threats to the City's strategic plan is essential to ensuring risk management controls add value to the risk management process. Failure to define the City's threat landscape may result the inability to protect against and respond in the instance where an event occurs. Disruptions in technology and unmitigated risks may prevent or delay residents from receiving vital services. We reviewed the Palo Alto IT Strategy FY19-FY21 and found that critical assets have been identified, prioritized and the strategy has been communicated to employees. However, employee responsibilities and action plans have not been identified, a risk appetite has not been established and Key Performance Indicators (KPI) and metrics to evaluate the achievement of strategic objectives and outcomes of the plan were not developed. We recommend The City establish its risk appetite and tolerance when developing strategy. Implementing a proactive IT risk management process is critical because the IT Departments provides numerous technology needs Citywide for Palo Alto. The strategy should be communicated to all stakeholders to ensure there is an understanding of their respective risk management roles and responsibilities. Critical assets should be identified and prioritized to determine what services and products are necessary for service delivery. An effective IT strategy can bring many benefits to an organization, including lower costs, greater control, more efficient and effective use of resources, and overall better strategic alignment and risk management.	IT / All Departments	Concurrence: Agree Target Date: FY22 Action Plan: IT is in the procurement process with a third party that will assist in developing a new three-year IT strategy that will include a risk management framework. The process will involve all departments to identify critical services and software required for service delivery. IT has based current and future risk management practices on COBIT (Control Objectives for Information and Related Technology). IT will adopt a Risk Management framework as a guideline that conforms to the city's requirements.
Finding: Step 2: Risk Identification and Assessment		
Risk Identification and Assessment includes establishing techniques for risk identification with consideration for vulnerabilities, decompose areas of concern and threats into statements of risk and compare to current risk register. Preemptively, assessing the loss-event scenarios that can impact the entire City is a proactive approach that is essential during the risk management process. Failure to identify historical, present and emerging risks may result in reduced confidence or visibility into any risks that can impede the City's ability to meet its objectives.	IT	Concurrence: Partially Agree Target Date: FY 22 Action Plan: IT requires a Business Impact Assessment (BIA) and Vendor Information Security

Recommendation	Responsible Department(s)	Agree, Partially Agree, or Do Not Agree and Target Date and Corrective Action Plan
The City does have operational level controls and processes to identify specific vulnerabilities. However, the City does not have an overall formal risk identification process, risk register or risk assessment process. Due to the lack of risk register, Baker Tilly conducted numerous interviews with key IT staff and end-users in each IT functional area to gain insight into the IT environment. The purpose of the interviews was to gain a general understanding of the controls in place to mitigate the associated risks within each IT area. Through these interview discussions and review of documentation we developed the IT Risk Matrix in Appendix A and identified opportunities for the City to further improve upon and reduce risk within IT operations. Information on the specific risk observations are included in Appendix C. We recommend The City develop a criteria to identify risk. Inputs include an inventory of the vulnerabilities, processes, assets, and groups of people in an organization so that consideration can be given to potential for adverse impacts. Risk identification and categorization can occur through many methods such as Strength, weakness, opportunity and threat (SWOT) analyses, Business impact analyses (BIA), Scenario analysis and Risk and control self-assessments (RCSA). Each method provides an opportunity to consider potential events that may prevent the achievement of business objectives. Then decompose the areas of concerns into a statement of risk and capture the conditions or situation that causes the concern, and an impact statement that describes the outcome of the realized risk. After these exercises, the register can be continuously compared against the risk statements on an on-going basis.		Assessment (VISA) are completed on new technology contracts and for renewal of existing technology contracts. In addition, IT has implemented a risk register for IT projects and plans to create a city-wide risk register to monitor impacts on-going. If council directs staff to move forward with the recommendation, staff will initiate a solicitation to contract with a third party to develop and implement a Risk Management Framework.
Finding: Step 3: Risk Analysis and Business Impact Evaluation		
Risk Analysis and Business Impact Evaluation includes developing a set of enterprise criteria to rank and rate risk and assign disposition to accept, avoid, mitigate or transfer risk based on the related actions. An IT risk management best practice framework of choice should be leveraged as guidance when conducting a risk analysis to facilitate the establishment of a risk disposition. Failure to rank, rate and take a positon on how to address risk may prevent the City's ability to respond to the most sensitive and critical events timely. The City has not undertaken efforts for rating and ranking risks or conducting a business impact evaluation. A Citywide criteria has not been established based on an IT risk management framework. Important events and near misses around IT affecting the City are not identified, analyzed and risk-rated. Risk assessments are not performed on a recurrent basis, using qualitative and quantitative methods that assess the likelihood (probability) and impact of	IT / CMO / All Departments	Concurrence: Partially Agree Target Date: FY23 Action Plan: To evaluate and rank the risk of technology solutions, a Business Impact Assessment (BIA) and Vendor Information Security Assessment (VISA) are required for new technology contracts and renewal of existing technology contracts. IT agrees that

Attachment: OCA - IT Risk Management - Final Draft (REDACTED) (13556 : Information Technology Risk

Recommendation	Responsible Department(s)	Agree, Partially Agree, or Do Not Agree and Target Date and Corrective Action Plan
identified risk. As a result, Baker Tilly also assigned likelihood and impact ratings to each IT risk area within the Risk Matrix in Appendix A, and plotted them on a Risk Heat Map, included in Appendix B. We recommend the City develop their own criteria for ranking the risks included in the risk analysis. The analysis should encompass first identifying threats to the City and then determining their likelihood, frequency and magnitude on the City. Then Citywide risk scenarios can be identified and analyzed. After analysis, the City can choose a risk disposition to address risk and the related scenarios based on the stated thresholds and/or events that are deemed unacceptable.		improvements to the process will be beneficial to analyze and rank risk effectively. If council directs staff to move forward with the recommendation, staff will initiate a solicitation to contract with a third party to develop and implement a Risk Management Framework.
Finding: Step 4: Risk Response		
Risk Response includes assigning a risk disposition (i.e. response), periodic reevaluation, assigning responsibility for response, and developing a risk mitigation and contingency plan. A disposition of accept, avoid, mitigate or transfer is usually assigned to each risk. Establishing actionable steps, assigning ownership and developing a formal risk response plan is critical to the risk management process. Failure to establish a process for responding to risk may result in the inability to mitigate risk timely due to a lack of resources and poor planning. The City does have a security incident response process where ownership is assigned, response plan is identified/implemented with oversight, and incident records are documented and retained. However, overarching IT risk management response procedures have not yet been implemented. Additionally, risk action plans are not developed and therefore do not allow for proper monitoring to ensure implementation, identification of costs, benefits, responsibility and approval of remedial actions or acceptance of residual risk. For proper risk response, management should internally review and select a disposition to address each risk. Per the Risk IT Framework, “Effective risk management requires mutual understanding between IT and the business regarding which risk needs to be managed and why.” An owner or responsible personnel should be identified for each risk and as conditions and the IT environment changes, the disposition should be revisited. A risk mitigation plan including mitigation activities, milestones and target completion date needs to be developed. Plan should also consider technology risk scenarios from a top-down or bottom-up approach, which both evaluate capabilities, timing, people, processes and physical infrastructure. Top-down begins	IT / All Departments	Concurrence: Agree Target Date: FY23 Action Plan: The Business Impact Assessment (BIA) and Vendor Information Security Assessment (VISA) processes identify risks. IT reviews the findings with the departments to ensure alignment. IT agrees a right-sized risk response and management practice is required taking into consideration budget and resources. If council directs staff to move forward with the recommendation, staff will initiate a solicitation to contract with a third party to develop and implement a Risk Management Framework.

Recommendation	Responsible Department(s)	Agree, Partially Agree, or Do Not Agree and Target Date and Corrective Action Plan
with a high-level view of mission and strategy; whereas Bottom-up begins with critical assets, application or systems across the City. In the event internal mitigation is too costly, a contingency plan can be established to minimize the risk impact.		
Finding: Step 5: Risk Reporting and Communication		
Risk Reporting and Communication includes on-going monitoring of risk status, periodic reevaluation and progress reporting to all relevant stakeholders. Once an IT risk management plan is in place, it is important to continuously communicate the status to all involved stakeholders to ensure the plan is adequate to meet the needs of the current IT environment. The inability to communicate the current state of risks timely may prevent senior management from being able to respond appropriately. Additionally, a lack of engagement may produce incomplete or ineffective mitigation efforts due to excluding stakeholder feedback when revisiting, reassessing and updating the plan based on ever-changing Citywide internal and external risk factors. Palo Alto does have periodic reporting to City Council related to budget and large Citywide projects. However, there is no formal process for IT Management and City Council's regular and routine consideration, monitoring and review of IT risk management. We recommend Palo Alto establish a risk reporting structure. Risks should be identifiable, recognized, well understood and known and managed through application of appropriate resources. This ensures there is a common understating of the City's risk exposure and increases transparency into the threat defenses the City has at its disposal. Risk should be monitored and risk mitigation plans updated as conditions change, if needed. To effectively report on risks, there should be a clear understanding and training, as needed, on the City's risk management strategy and any related policies and procedures. Any areas where the City's current capabilities are lacking should be communicated so that the necessary resources can be obtained to enhance the risk management process expeditiously. Once the risks have been identified, status reporting should include the risk profile, Key Risk Indicators (KRIs), event/data loss, a root cause analysis and migration options. Per the Risk IT Framework, "Information must be communicated at the right level of detail and adapted for the audience."	IT / All Departments	Concurrence: Agree Target Date: FY23 Action Plan: IT agrees the desired outcome is to adopt and implement a mature Risk Management Framework that fits the city's requirements and provides reports to the proper management level, considering budget and resources. If council directs staff to move forward with the recommendation, staff will initiate a solicitation to contract with a third party to develop and implement a Risk Management Framework.

City of Palo Alto (ID # 13604)

Policy and Services Committee Staff Report

Report Type: Action Items **Meeting Date: 10/12/2021**

Title: Review and Approval of the Office of the City Auditor (OCA) Annual Report

From: City Manager

Lead Department: City Auditor

In accordance with Task 5 of our agreement with the City, Baker Tilly is required to report annually on a variety of topics, generally including progress to plan.

The Office of the City Auditor (OCA) has drafted a written Annual Report, generally covering the OCA's progress to plan. The below summarizes progress as organized by Baker Tilly's agreement with the City (i.e., by Task). Highlights in the report and in the oral presentation include the following:

- Task 1 – City Wide Risk Assessment
  - Presented to and Approved by P&S on February 9, 2021
  - Presented to and Approved by City Council on March 1, 2021
- Task 2– Prepare an Annual Audit Plan
  - Presented to and Approved by P&S on February 9, 2021
  - Presented to and Approved by City Council on March 1, 2021
- Task 3 – Assist in Managing the Financial Audit
  - FY20 Audit Presented to and Approved by Finance Committee on December 1, 2020
  - FY20 Audit Presented to and Approved by City Council on January 11, 2021
  - Single Audit Report Presented to and Approved by City Council on May 10, 2021
- Task 4 – Execute Audit Plan
  - Kicked-off Nine (9) of Ten (10) Approved Task Orders
  - Completed Field Work for Five (5) Projects
  - One (1) Report Presented to and Approved by Policy & Services
  - Three (3) Reports Pending Presentation to Policy & Services in October/November 2021
- Task 5 – Periodic Reporting and Hotline Monitoring
  - Closed Two of Two (2/2) Hotline Reports Received in CY21

    - Presented Quarterly Reports
    - Perform Follow-up Activities on Prior Audit Findings and Corrective Action Plans
    - Participated in Various Meetings, Including City Council, Executive Leadership, Agenda Planning, and Committee Meetings
- Task 6 – City Auditor evaluation
    - N/A – To Be Completed in FY22

Discussion

The attached report summarizes the OCA's progress to plan as well as progress on corrective action plans for prior audit findings for audit activities completed in FY18-FY20.

Timeline, Resource Impact, Policy Implications

The annual report does not have timeline, resource impact, or policy implications.

Stakeholder Engagement

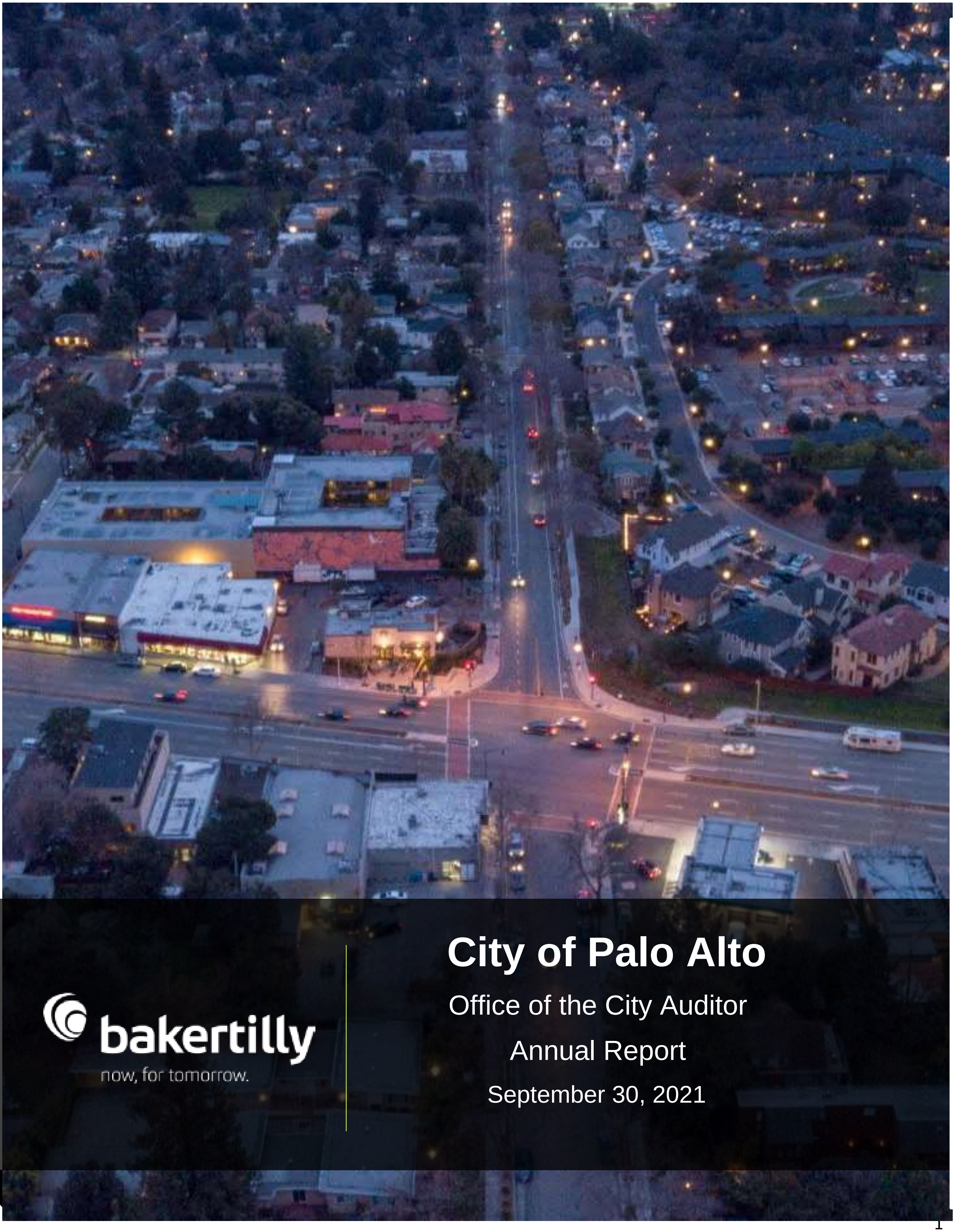
The Office of the City Auditor worked primarily with City Manager's Office and Executive Leadership to obtain updates on implemenation of corrective action plans in response to prior audit findings.

Environmental Review

Environmental review is not applicable to this activity.

Attachments:

- OCA - Annual Report (FINAL DRAFT)



bakertilly
now, for tomorrow.

City of Palo Alto

Office of the City Auditor

Annual Report

September 30, 2021

Introduction

The City Auditor is appointed by and reports functionally to the City Council. The City Charter defines the City Auditor's important role and furthers the City Council's commitment to internal auditing, transparency, and accountability in government. The Office of the City Auditor (OCA) conducts audits and reviews including reviews of the effective and efficient use of resources, internal control systems, and compliance with policies, procedures, and regulatory requirements.

The Palo Alto City Council approved a contract through June 2022 with an option to extend for three years with advisory, tax, auditing, and assurance firm Baker Tilly US, LLP (Baker Tilly) and appointed Kyle O'Rourke, MPA, CIA, CGAP, CRMA, Principal in Baker Tilly's Public Sector practice, as City Auditor on September 28, 2020. This report is intended to communicate our accomplishments over the first year of our work.

Accomplishments

Per City Council direction on February 10, 2020, the City Council Appointed Officers (CAO) Committee oversaw a request for proposals (RFP) process for outsourced internal auditing services, led a procurement process aligned with City Council direction, and engaged in a transparent review of scope of work services, RFP evaluation, and a public interview process as part of the overall effort. Following these public interviews, the City Council conducted closed session interviews of the City Auditor candidates designated by the top firms recommended by the CAO Committee.

Through the RFP process and interviews, the City Council selected Baker Tilly and Kyle O'Rourke to lead the City's internal audit services. Kyle O'Rourke was appointed as Palo Alto's City Auditor in conformance with the Palo Alto City Charter (Contract No. C2117934).

Risk Assessment & Audit Plan Development

In its capacity serving as the City Auditor function, and in accordance with Baker Tilly's agreement with the City, Baker Tilly performed a citywide risk assessment. The purpose of the assessment was to identify and prioritize risks in order to develop the annual audit plan. During the risk assessment, Baker Tilly assessed a wide range of risk areas, including strategic, financial, operational, compliance, technological, and reputation risks. The results of the assessment were transmitted to the full City Council for public review and was approved by the Policy and Services Committee on February 9, 2021 (Report 11952).

On March 1, 2021, the Risk Assessment Report and Annual Audit Plan were approved by City Council (Report 12022). At that time, eight (8) task orders were approved for execution. At a subsequent meeting on May 10, 2021, two (2) additional task orders were approved for execution (Report 12110).

Attachment: OCA - Annual Report (FINAL DRAFT) (13604 : Office of the City Auditor Annual Report)

Execution of the Audit Plan

Between March and September 2021, Baker Tilly has formally kicked off nine (9) of ten (10) approved audit activities, including those listed below:

- Construction Project Controls
- Public Safety Building Construction
- Asset Capitalization
- Assessment of SAP Functionality and Internal Controls
- Information Technology Risk Management
- Power Purchase Agreement
- Economic Recovery Advisory
- Building Permit & Inspection Process
- Nonprofit Agreements Risk Management

The current status of each audit activity, as of September 30, is highlighted on the following page.

Function	Project Title	Audit Objectives	Status	Detail
Public Works	Construction Project Controls Assessment	• Identify key processes and controls in the construction project management program. • Assess the control environment and make recommendations for improvement.	Report Drafted	Report is drafted and i under review by proce owners, CMO, and the City Attorney's Office.
Public Works	Construction Audit – Public Safety Building	• Assess the control environment and make recommendations for improvement. • Establish monthly procedures to evaluate project billing and analyze change orders, and evaluate other key risk areas.	In Progress	First monthly monitorir memo to be delivered November P&S
Administrative Services	Asset Capitalization Audit	• Identify the cause of the $12.6M capital asset adjustment made during FY2020 by evaluating the process to record and report the costs associated with CIP • Determine whether adequate controls are in place to ensure that costs associated with CIP are properly categorized and recorded in accordance with the accounting policy and relevant accounting standards	Report Drafted	Final Draft Report was presented at the Augu 10, P&S meeting (Report 13461) and wi be presented to Counc for consent.
Information Technology	Assessment of SAP Functionality and Internal Controls (FY21)	• Participate as an advisor to the project steering committee for Phase 2 of the ERP system upgrade. • Evaluate internal control design as system configuration is analyzed.	Report Drafted	Report is drafted and i under review by proce owners, CMO, and the City Attorney's Office.
Information Technology	IT Risk Management Assessment	• Identify key risks and controls within the IT function – including IT governance and IT security. • Evaluate the adequacy of the control environment and offer recommendations for improvement.	Report Drafted	Report to be presentec at the October 12 P&S meeting.
Utilities	Power Purchase Agreement Review	• Evaluate the process for evaluating and entering into power purchase agreements. • Assess the effectiveness of internal controls in the management of the power purchase agreements and accuracy and compliance of billings.	Report Drafted	Report is drafted and i under review by proce owners, CMO, and the City Attorney's Office.
Administrative Services	Economic Recovery Advisory	• Review the City's long-term financial planning model and offer recommendations for improvement. • Identify and evaluate key revenue source categories that present long term risk to the City's financial sustainability and perform scenario analysis. • Offer ad hoc advisory assistance during the FY22 budget process.	In Progress	Formal kick-off took place in September 2021.
Planning	Building Permit & Inspection Process Review	• Identify highest impact area to focus the assessment (e.g., specific permit type(s), specific sub-processes, etc.). • Document corresponding process(es) and evaluate for efficiency and effectiveness. • Benchmark operational performance against industry practices and established standards.	In Progress	Reviewing data requested in August.
Citywide	Nonprofit Agreements Risk Management Review	• Evaluate controls in place to ensure that nonprofit organizations are properly vetted prior to selection and monitored through the life of an agreement. • Assess the performance monitoring process against the best practice. • Follow up on relevant audit findings from past audit work.	In Progress	In the fieldwork phase this audit activity.
Utilities	Work Order Process and Accounting Review	• Perform an initial assessment to identify high risk subprocesses in the work order process (e.g., labor, materials, specific utility). • Document and evaluate the processes and controls in place to ensure proper recording of costs. • Perform tests to determine the accuracy of attributed costs for a sample of completed work orders.	Awaiting Task Order Signature	The Task Order will be provided to P&S on October 12th for review and approval.

The OCA proposed multiple other audit activities to be commenced in FY22. Those audit activities include:

- Investment management
- Application Lifecycle Management
- SAP Functionality and Internal Controls (Phase 2)
- Wastewater Treatment Plant Agreement

The OCA will complete the FY22 risk assessment and audit planning process in order to determine if the above list continue to be priorities for the OCA.

Financial Audit Coordination

The OCA is tasked with assisting in the management of the external financial audit. Given the timing of the contract approval, the majority of the fieldwork for the FY20 audit was completed prior to Baker Tilly's engagement with the City. In FY21, Baker Tilly assisted in presenting the financial audit results for FY20.

On December 1st, Macias Gini O'Connell LLP (MGO) presented the following audit reports to the Finance Committee for review and approval (Report 11741):

- Auditor's Report to the City Council (the "Management Letter")
- Cable TV Franchise, Independent Auditor's Report and Statements of Franchise Revenues and Expenses for the Years Ended December 31, 2018 and 2019
- Palo Alto Public Improvement Corporation Annual Financial Report for the Year Ended June 30, 2020
- Regional Water Quality Control Plant Independent Auditor's Report and Financial Statements for the Year Ended June 30, 2020
- Independent Accountant's Report on Applying Agreed-Upon Procedures Related to the Article XIII-B Appropriations Limit for the Year Ended June 30, 2020

City Council subsequently approved the financial audit reports listed above on January 11, 2021 (Report 11880).

The Single Audit report was presented to the Finance Committee an approved on April 6, 2020 (Report 12107) and was approved by City Council on May 10, 2021 (Report 12108).

The contract with MGO was set to end with the completion of the FY20 external financial audit activities. Given the extraordinary circumstances of the COVID-19 Pandemic, the OCA initiated an exception to competitive solicitation in order to extend the contract to cover one additional year – the FY21 financial audit activities. The contract amendment to extend the MGO contract was approved by City Council on April 12, 2021 (Report 12106).

As of September 2021, the external financial audit for FY21 is underway and is expected to be completed for delivery to the Finance Committee in December 2021. Additionally, the OCA is working with Administrative Services to issue a Request for Proposals (RFP) for external financial audit services beginning at the conclusion of FY22.

Monitoring of Prior Audit Findings

The City Auditor is responsible for monitoring prior audit findings and verifying whether corrective actions have been implemented as planned and approved by City Council. The OCA reviewed prior audit reports from FY18-FY20 in order to follow up on the audit findings and corrective actions. Note that all reports were the work of the prior in-house City Auditor. Moving forward, the OCA will continue to monitor whether corrective actions are implemented as described by the auditee during the close out of our audit activities. The findings, corrective action plans, and current status to those audit reports are summarized on the following pages.

Attachment: OCA - Annual Report (FINAL DRAFT) (13604 : Office of the City Auditor Annual Report)

Prior Audit Findings – FY18-FY20

Audit Report	Report Date	Finding	Recommendation	Responsible Department(s)	Initial Management Response (upon audit completion)	Current Status As of 9/30/21	Implementation Update As of 9/30/21
Accuracy of Utility Water Meter Billing Audit	08/16/17	Finding 1: CPAU has not adequately prevented, detected, nor corrected water meter billing errors.	1.1. Correct the billing errors identified.	Utilities	**Concurrence:** Agree **Target Date:** November 2017 **Action Plan:** Utilities staff is confirming the specific addresses and errors cited in the audit. Staff will then take immediate actions to rectify the overcharge situation by contacting the customers and updating their accounts with the correct meter charge as well as reconciling the incorrect charges for the past three years. For the undercharge or backbill scenario, staff plans to recommend City Council approval to modify current meter billing policy and eliminate mandated customer backbilling for utility-caused metering errors under certain circumstances.	Completed	The billing errors identified were corrected in August 2017. Council approved on 4/2/2018 ID# 9024, updated Utility Rule and Regulation 11 to include in Section I as a new section 4: "When CPAU is the cause of an error that results in an overcharge, CPAU will refund the full amount of the overcharge, subject to the three year retroactive billing adjustment period described above. Back bills for undercharges will be calculated and approved by the Director of Utilities, or delegate, and may be waived over $500 per Customer Account, per incident, subject to the three year retroactive billing adjustment period described above."
Accuracy of Utility Water Meter Billing Audit	08/16/17	Finding 1: CPAU has not adequately prevented, detected, nor corrected water meter billing errors.	1.2. Investigate each of the 123 water meters that do not match the meter purchasing record, determine if a record or billing correction is required, and correct accordingly.	Utilities	**Concurrence:** Agree **Target Date:** November, 2017 **Action Plan:** Staff has completed an initial inspection of the 123 meters in the field. Staff will need to conduct further investigation on a few of the accounts to confirm meter type, pipe connection size, and dial register. Thus far, staff has confirmed 84 water meters did not match the meter or billing record. Staff will take the necessary actions to rectify the overcharges and undercharges.	Completed	Staff completed the field inspection and the customer accounts were adjusted on November 2017.
Accuracy of Utility Water Meter Billing Audit	08/16/17	Finding 1: CPAU has not adequately prevented, detected, nor corrected water meter billing errors.	1.3. Review and correct the meter record errors identified for meter sizes larger than 2 inches.	Utilities	**Concurrence:** Agree **Target Date:** December 2018 **Action Plan:** In preparation for the new CIS Utility billing system and potential advanced meter deployment, staff will consider an in-house or contract service audit of the three metered services (electric, gas, water). Staff will also review and update as needed roles and responsibilities for key staff involved in ensuring meter accuracy, including procurement, inventory, testing, installation, and billing records management.	In Progress	Field audit work is completed and Staff will review the meter exceptions against the audit photos and perform a physical inspection if required. After verification, meter records will be updated accordingly. The contractor completed 99% of the field audit or approximately 73,100 electric, gas and water meters to validate and ensure accurate meter data. City staff will complete the field audit of the 900 non-accessible meters by the contractor. The project was delayed due to COVID-19 and field audits were completed by February 2021. **Expected completion date:** FY 2022

Attachment: OCA - Annual Report (FINAL DRAFT) (13604 : Office of the City Auditor Annual Report)

Audit Report	Report Date	Finding	Recommendation	Responsible Department(s)	Initial Management Response (upon audit completion)	Current Status As of 9/30/21	Implementation Update As of 9/30/21
Accuracy of Utility Water Meter Billing Audit	08/16/17	Finding 1: CPAU has not adequately prevented, detected, nor corrected water meter billing errors.	1.4. Explore options for addressing equity when making changes to customer meter size rates and establish a policy and process for determining, documenting, and notifying customers of changes to their meter size and, if appropriate, the rate change associated with the new meter size.	Utilities	**Concurrence:** Agree **Target Date:** July 2018 **Action Plan:** The audit's questioning of utility practices regarding changes to meter sizes is based on a unique situation that occurred 22 years ago and does not reflect current policy or process. The situation arising out of Southgate was a unique case and staff does not agree that this or other meter replacement practices raise equity issues. With regard to differential rates for different meter sizes, staff is currently reviewing policy options for addressing this issue going forward, and will develop options such as consolidating the fixed rate for 5/8" and 1" meters for consideration by the City Council.	Completed	Council approved on 4/16/2019 ID# 10149, staff updated to charge all residential customers with 5/8", 3/4", and 1" meters, which include fire flow, a uniform monthly service fee.
Accuracy of Utility Water Meter Billing Audit	08/16/17	Finding 1: CPAU has not adequately prevented, detected, nor corrected water meter billing errors.	1.5. With the understanding that CPAU will be migrating to a new ERP system: a) Implement a temporary monitoring or reporting system to identify record discrepancies that may result in billing errors and correct as discrepancies are identified b) Ensure the new ERP system will have automated controls in place to prevent such discrepancies and identify them if they do occur.	Utilities	**Concurrence:** Agree **Target Date:** December 2019 **Action Plan:** a. Staff has established a monthly reconciliation report to monitor and identify inconsistent billing and meter attributes which will ensure comprehensive detection of potential error sources across inventory, meter change activity, and billing databases. b. Elimination of redundant manual entry has already been identified as a system requirement for the new CIS system. Staff will monitor the ongoing procurement for a new customer information system and enterprise resource planning system to ensure system requirements continue to prioritize minimizing manual entry through integration across databases and automated data entry.	Completed	a) Completed - Reconciliation Report created and used periodically to identify any meter discrepancies in ERP/CIS system. b) Completed - In FY 2022, staff is working on the scope of work for the Phase 2 upgrade to the City's existing ERP system. This identified desired system requirement for new automated controls is included in this review process for potential final inclusion in the Phase 2 of the project. The implementation of a new ERP was cancelled and the City chose to remain on the current ERP platform with SAP. The City has completed a technical upgrade of the current ERP system and is planning a Phase 2 of this upgrade to leverage potential additional tools which is scheduled to be completed in FY 2023 - FY 2024.

Attachment: OCA - Annual Report (FINAL DRAFT) (13604 : Office of the City Auditor Annual Report)

Audit Report	Report Date	Finding	Recommendation	Responsible Department(s)	Initial Management Response (upon audit completion)	Current Status As of 9/30/21	Implementation Update As of 9/30/21
Accuracy of Utility Water Meter Billing Audit	08/16/17	Finding 2: CPAU has installed 1,178 water eMeters throughout the City' however, there are no testing standards, and the accuracy, performance, and reliability of these meters are uncertain.	2.1. Develop a policy and procedure to transparently report significant, systemic, infrastructure changes to City Council, and update any CPAU Rules and Regulations that may be outdated to current practice or affected by policy changes.	Utilities	**Concurrence:** Agree **Target Date:** Immediately**Action Plan:** Major infrastructure changes are presented to City Council for approval. However, standards are technical documents that provide the general conditions and specifications for the construction of the Water Gas and Wastewater System. Updates to standards are subject to multiple levels of professional review including engineering, procurement and legal. Updated standards will be communicated to City Council as informational when substantive.	Completed	The item was updated as complete and accepted by the Auditor's office on 6/11/2019. In collaboration with ASD, the following control processes are in place to transparently report changes: 1. Purchasing Policies and Procedures: a. Sole Source Standardization process; b. Contracts for professional services over $85,000 require Council approval 2. Utility Rule and Regulations 3. Meter and Specification Update 4. Utilities Engineering Electric and WGW Construction Standards
Accuracy of Utility Water Meter Billing Audit	08/16/17	Finding 2: CPAU has installed 1,178 water eMeters throughout the City' however, there are no testing standards, and the accuracy, performance, and reliability of these meters are uncertain.	2.2. Seek direction and approval from City Council before proceeding further with the future installation of eMeters or any electronic meters.	Utilities	**Concurrence:** Agree **Target Date:** Ongoing **Action Plan:** Procurement and installation of e-meters will remain suspended until adoption of an AWWA standard for testing and the availability of independent test resources (either in-house or contracted). It is expected that a final standard for testing of E-meters will be available at the end of 2017. The new standards are not expected to change the accuracy requirements from those expected of the positive displacement meter with the exception that there will likely be an extended range of accuracy for low flows. It should be noted the E-Meters is a specific product line, and mechanical meters may also have electronic components.	Completed	This item was updated as complete and accepted by the Auditor's office on 6/11/2019. The American Water Works Association (AWWA) standards for electromagnetic and ultrasonic water meters were published in October 2018. After staff's review and meeting with other water agencies and consultants, staff has decided not to install new ultrasonic water meters until the technology matures. At this time, Utilities will not be adopting the new electromagnetic and ultrasonic water meter standards. Utilities will notify Council in the future when Utilities adopt the new AWWA electromagnetic and ultrasonic water meter standards.

Audit Report	Report Date	Finding	Recommendation	Responsible Department(s)	Initial Management Response (upon audit completion)	Current Status As of 9/30/21	Implementation Update As of 9/30/21
Accuracy of Utility Water Meter Billing Audit	08/16/17	Finding 2: CPAU has installed 1,178 water eMeters throughout the City' however, there are no testing standards, and the accuracy, performance, and reliability of these meters are uncertain.	2.3. Determine if the 1,178 installed eMeters should be uninstalled and replaced with the original displacement meter and if billing adjustments are required.	Utilities	**Concurrence:** Agree **Target Date:** July 2018 **Action Plan:** All customers with e-meters installed will be immediately notified of this audit, and that additional information will be provided as available. For eMeter testing, staff will send a sampling of eMeters to independent testing companies to determine if they are performing per manufacturer specification, and based on these results will determine next steps. In addition, the Water Meter Shop has staffing challenges and does not currently have the resources required to undertake this replacement project. At this time, staff will continue to monitor the meter reads for irregularities of both the installed positive displacement and eMeters as part of the billing exception process. Staff is also developing a customer plan for addressing any accuracy concerns with the e-meters already installed.	Completed	This item was updated as complete and accepted by the Auditor's office on 6/11/2019. Staff hired a contractor to test a sampling of eMeters. The contractor tested the eMeters under four different scenarios. Overall, the testing results measured correctly within the manufacturer's specifications. Based on manufacturer's test results, third party sampled testing and monthly meter readings of eMeters, staff believes these meters are functioning properly and does not recommend replacing them until their end of life. Customer with eMeters were notified of the opportunity to replace the eMeters with positive displacement meters.
Accuracy of Utility Water Meter Billing Audit	08/16/17	Finding 3: Purchase of water eMeters did not conform to standardization and sole source policies, and eMeter expenditures were not monitored.	3.1. ASD Purchasing to clarify its purchasing policy and procedures for new and renewals of product standardization and sole source.	ASD	**Concurrence:** Agree **Target Date:** December 2017 **Action Plan:** Staff will update the policy and coordinate with stakeholders to ensure the policy is clear and easy to follow. Staff will then finalize the policy and disseminate to departments.	In Progress	This has been implemented and is part of the standard procedures for sole source and standardization requests. In FY 2022, by the close of the 3rd Quarter staff expect to have the formal policy drafted and finalized updating the purchasing manual standardization and sole source section as well as any necessary forms. For Standardization Requests (new & renewals), the requesting department creates a PR and submits Appendix E Form for a standardization request. Once the standardization request is approved, the Purchasing department files a copy and the requesting department receives a copy. In addition to requesting an approval for standardization, the requesting department also submits the Appendix E form for a sole source when procuring the standardized product if not available by multiple distributors. The approved sole source is filed with Purchasing in the Master Library under exemptions and a copy provided to the requesting department. Expenditures for Standardize products (sole source or not) are manually tracked by Purchasing. **Expected Completion Date:** FY 2022 Q4

Audit Report	Report Date	Finding	Recommendation	Responsible Department(s)	Initial Management Response (upon audit completion)	Current Status As of 9/30/21	Implementation Update As of 9/30/21
Accuracy of Utility Water Meter Billing Audit	08/16/17	Finding 3: Purchase of water eMeters did not conform to standardization and sole source policies, and eMeter expenditures were not monitored.	3.2. ASD Purchasing to retrain appropriate ASD and CPAU staff on Purchasing policies and procedures, and completion of required forms.	ASD	**Concurrence:** Agree **Target Date:** January 2018 **Action Plan:** In conjunction with 3.1 staff will provide training.	Completed	The business process has been updated, see the current process in recommendation 3.1, and is currently in place citywide.
Accuracy of Utility Water Meter Billing Audit	08/16/17	Finding 3: Purchase of water eMeters did not conform to standardization and sole source policies, and eMeter expenditures were not monitored.	3.3. ASD Purchasing to determine roles and responsibilities and develop a procedure for tracking Sole Source purchases to prevent the overspending of approved amounts.	ASD	**Concurrence:** Agree **Target Date:** March 2018 **Action Plan:** The SAP system does not currently provide an automated check on sole source spending. Staff will evaluate whether the system can be configured to allow for this. If not, staff will implement manual procedures to track sole source spending.	Completed	Staff has implemented a manual procedure for tracking expenditures for standardized products (sole source or not) on a document by the Purchasing staff. The current business process also ensures that sole source form requires a PR for funding and processing, thereby creating a record and authorization amount in the ERP system as well.
Overtime Audit	09/06/17	Implementing a continuous monitoring process for overtime in the new Enterprise Resource Planning (ERP) environment can help the City improve its resource allocation and utilization.	1. Explore the potential of developing a continuous monitoring process to provide more detailed information on overtime usage so that management can better manage and control overtime costs. A continuous monitoring system could include data analytics to extract data on service demands, absences and vacancies, and elements of city policies and contractual requirement that could be useful in identifying opportunities to reduce overtime costs.	ASD	**Concurrence:** Agree **Target Date:** 4th Quarter 2018 **Action Plan:** ASD will work with departments to explore the potential of developing a continuous monitoring process for overtime.	Completed	Staff has implemented a business process to provide departments citywide with routine financial monitoring reports for revenues and expenses in the City's General Fund. This report, sent at least monthly, provides budget to actual comparisons as well as multiple potential forecasts based on routine models such as historic trends to assist in better management of costs, including overtime. Departments are responsible for the monthly monitoring of expenditures and quarterly financial status reports continue to be provided to identify any areas of concern throughout the year. The implementation of a new ERP was cancelled and the City chose to remain on the current ERP platform with SAP. The City has completed a technical upgrade of the current ERP system and is planning a Phase 2 of this upgrade to leverage potential additional tools which is scheduled to be completed in FY 2023 - FY 2024. As part of this phase 2, staff will include this as a desired change, if feasible and cost effective.

Attachment: OCA - Annual Report (FINAL DRAFT) (13604 : Office of the City Auditor Annual Report)

Audit Report	Report Date	Finding	Recommendation	Responsible Department(s)	Initial Management Response (upon audit completion)	Current Status As of 9/30/21	Implementation Update As of 9/30/21
Overtime Audit	09/06/17	Implementing a continuous monitoring process for overtime in the new Enterprise Resource Planning (ERP) environment canhelp the City improve its resource allocation and utilization.	2. Form a work group consisting of main end users and stakeholders to design shared system capabilities and standardized overtime management processes in the new ERP environment by: • Identifying useful overtime data including their source, and user interface (e.g., dashboard with drilldown and reporting capabilities) that allow users to analyze pertinent overtime factors shown in Appendix 1 in a comprehensive manner. • Identifying manual data collection and auxiliary processes (e.g., billing, reimbursement) that can be automated. • Reviewing applicable ERP system requirements to ensure needed capabilities are included in the City's ERP contract.	ASD	**Concurrence:** Agree**Target Date:** 4th Quarter 2018**Action Plan:** ASD will work with departments to determine shared needs for overtime in the new ERP system. Staff is currently evaluating ERP solutions for payroll and core financials and staff has communicated the important of overtime reporting to the vendors. Once an ERP solution is selected staff will finalize overtime reporting requirements and build those requirements into the new ERP system with the implementation consultants.	Completed	Staff has implemented a business process to provide departments citywide with routine financial monitoring reports for revenues and expenses in the City's General Fund. See recommendation #1 for this item for current manual process.
Business Registry Audit	08/28/18	The City's business registry data was not reliable. Data that MuniServices LLC started collecting under contract with the City in 2018 should be more reliable, but there is opportunity for further improvement.	1. Identify and consult with key stakeholders (e.g., City Council, Planning and Community Environment Department) who use the business registry to clarify existing and potential uses and priorities for business registry data. Based on these consultations, review and modify the questions, as necessary that the City asks businesses to self-report.	City Manager's Office, Development Services, Planning and Community Environment, and Transportation	**Concurrence:** Agree **Target Date:** June 30, 2019 **Action Plan:** Development Services Department (DSD) will lead an effort to gather feedback from internal department stakeholders as noted in the column to the left. The department may also discuss the registry with external stakeholders. Staff will return to City Council for a recommendation prior to the 2020 Business Registry cycle.	On-Hold	The City Council paused collection of the BRC fees due to COVID-19 and the impact on businesses in the community. The Council has also actively reviewing scenarios for a potential November 2022 local ballot measure, specifically on impacting business; the decision on this potential tax measure will impact the priorities for the BRC program moving forward. Staff supporting this program has been vacant and therefore significantly impacting capacity to both address changes to this program and support the pursuit of a local ballot measure. **NOTE:** In FY 2020, the Business Registry Certificate (BRC) program was reallocated from the former Development Services Department to the Administrative Services Department with the merging of the Development Services Department and the Planning and Community Environment Department. This function specifically was determined to best be placed in Administrative Services where the majority of taxes and administrative fees are handled by various teams with the Treasury Division of the department. **Expected completion date:** TBD

Attachment: OCA - Annual Report (FINAL DRAFT) (13604 : Office of the City Auditor Annual Report)

Audit Report	Report Date	Finding	Recommendation	Responsible Department(s)	Initial Management Response (upon audit completion)	Current Status As of 9/30/21	Implementation Update As of 9/30/21
Business Registry Audit	08/28/18	The City's business registry data was not reliable. Data that MuniServices LLC started collecting under contract with the City in 2018 should be more reliable, but there is opportunity for further improvement.	2. As part of a broader strategy to improve the reliability of the business registry, explore and assess the cost versus benefit of the following options, which may work in synergy: • Identify the type and sources of external data that can improve the accuracy of data collected. This could include, for example, using the U.S. Census Bureau's Statistics of U.S. Businesses program data, either by itself or together with other available data, to validate business registry data and identify potentially unregistered businesses. • Provide City data to MuniServices to help improve and monitor the reliability of the registry data (e.g., validation of registration when code violations are reported against a business or when a business applies for a permit, utilities customer data). • Gather data from in-person observations of City businesses. If the City decides to conduct in-person observations, it should work with MuniServices to plan, conduct, and accurately record the observations in a useful format. Alternatively, this could include hiring temporary help to physically identify where businesses are located in the	ASD	**Concurrence:** Agree **Target Date:** June 30, 2019 **Action Plan:** DSD agrees to explore and assess the cost versus the benefit of the suggested options. Staff will return to the City Council during the Fiscal Year 2020 budget cycle with any associated program recommendations. Staff does intend to utilize MuniServices business discovery and analytics services prior to the 2019 Business Registry cycle. This service will utilize external sources acquired by MuniServices. Staff will also meet with the Utilities and Information Technology departments to discuss data sharing.	Completed	As noted above, the BRC program was reallocated to the Administrative Services Department in FY 2020. **June 2020 Management Update (CMR: 11111)** The verification of business data is done through the discovery process performed by Avenu Insights & Analytics. City Council approved a new contract with Avenu Insights & Analytics on 12/2/19 (CMR #10493) that included ways for increasing the accuracy of BRC data. This contract outlined Avenu Insights & Analytics using resources such as their own proprietary database sources, the State of California Sales Tax data, Santa Clara County Real Property data, Dun & Bradstreet, and InfoUSA for verifying the accuracy of the BRC database. Data sources used varies by availability and coverage area. Additionally, to begin discovery services, the contract states Staff provides business fee and business and occupation application forms as well as database files such as commercial utility billing records to Avenu Insights & Analytics. The Palo Alto Transportation Management Association (PATMA) provided staff with business data gathered through in-person observations of downtown businesses to assist in keeping the BRC database accurate. This was provided to the Avenu Insights & Analytics discovery services team to inform their efforts. Staff will explore the future of making this a regular source of information provided.

Audit Report	Report Date	Finding	Recommendation	Responsible Department(s)	Initial Management Response (upon audit completion)	Current Status As of 9/30/21	Implementation Update As of 9/30/21
			City to supplement data self-reported by businesses or through other data sources and to improve the accuracy of future updates.				
Business Registry Audit	08/28/18	The City's business registry data was not reliable. Data that MuniServices LLC started collecting under contract with the City in 2018 should be more reliable, but there is opportunity for further improvement.	3. Update the Development Services business registry administrative manual to reflect Development Services' new project management and contract administrator roles and responsibilities. The update should incorporate: • The City's guidelines for contract administration roles and responsibilities that are available in the City's Procurement Fundamentals Training Guide. • Specific steps to monitor the reliability of the registry data. This can include basic steps to periodically review trends and validate the consistency, accuracy, and completeness of a	ASD	**Concurrence:** Agree **Target Date:** December 31, 2018 **Action Plan:** DSD will update the administrative manual prior to the 2019 Business Registry Cycle. Staff does intend to review reliability of the registry data prior to the launch of each annual collection cycle and to include reference to this practice in the administrative manual.	On-Hold	The City Council paused collection of the BRC fees due to COVID-19 and the impact on businesses in the community. The Council is also actively reviewing scenarios for a potential November 2022 local ballot measure, specifically on impacting business; the decision on this potential tax measure will impact the priorities for the BRC program moving forward including the administration. Staff supporting this program has been vacant and therefore significantly impacting capacity to both address changes to this program and support the pursuit of a local ballot measure. **NOTE:** In FY 2020, the Business Registry Certificate (BRC) program was reallocated from the former Development Services Department to the Administrative Services Department with the merging of the Development Services Department and the Planning and Community Environment Department. This function specifically was determined to best be placed in

Attachment: OCA - Annual Report (FINAL DRAFT) (13604 : Office of the City Auditor Annual Report)

Audit Report	Report Date	Finding	Recommendation	Responsible Department(s)	Initial Management Response (upon audit completion)	Current Status As of 9/30/21	Implementation Update As of 9/30/21
			sample of registry records by comparing them with other City or publicly available databases.				Administrative Services where the majority of taxes and administrative fees are handled by various teams with the Treasury Division of the department. **Expected completion date:** TBD
ERP Planning: Data and System Governance	06/13/18	Finding 1: Better information technology governance can help ensure that IT systems, including the new ERP system, support City goals, and objectives	1.1. Assign roles and responsibilities for IT governance (e.g., "chief governance officer") to an existing City position that reports or could potentially report directly to the City Manager or the Chief Information Officer. The roles and responsibilities should include: ● Ensuring that City departments and stakeholders who are the users of the City's information systems are included in governance processes and decision making, including decisions to address security risks. • Ensuring that there is a process to validate the accuracy and completeness of key IT reports that are used in decision making or reporting (e.g., the City's document that shows decisions on addressing risks identified in the Coalfire report; decisions regarding departmental roles and responsibilities for the new ERP system).· Ensuring that governance covers all key	Information Technology	**Concurrence:** Agree**Target Date:** December 31, 2019**Action Plan:**The IT Department implemented IT Governance citywide in 2012 and since then it has been rightsized to reflect the evolving needs of the City.The roles and responsibilities for a leader in IT governance have already been assigned to an individual who reports to the Chief Information Officer (CIO).The IT Department agrees that work is required to address gaps in our city IT governance processes today including leadership roles, communications, reporting, and decision-making.	Closed	As outlined in the audit, the Information Technology Department (ITD) does have citywide governance in place and assigned to staff. This recommendation has been superseded by the ITD Risk Assessment and recommendations within as completed by Baker Tilly in October 2021. This updated assessment extends beyond this identified ITD scope to a broader citywide perspective.

Audit Report	Report Date	Finding	Recommendation	Responsible Department(s)	Initial Management Response (upon audit completion)	Current Status As of 9/30/21	Implementation Update As of 9/30/21
			aspects of the City's information systems (e.g., ensuring that the IT Department has policies and procedures to address the use, organization, security, and access rights for the City's network drive).				
ERP Planning: Data and System Governance	06/13/18	Finding 1: Better information technology governance can help ensure that IT systems, including the new ERP system, support City goals, and objectives	1.2. Adopt an industry standard IT Governance frameworks, such as COBIT, and a process assessment and rating or maturity model, such as the COBIT 5 process assessment model. Create a plan to achieve a process capability model of 3 (i.e., "established") or higher for: • IT staffing and funding • IT governance roles and responsibilities • Aligning IT with departments' priorities • Measuring and monitoring IT governance outcomes · Identifying and mitigating IT risks	Information Technology	**Concurrence:** Agree. **Target Date:** December 31, 2019 **Action Plan:** IT Department agrees to identify and adopt an appropriate, rightsized, industry-recognized, IT governance framework. The IT Department working with the City Manager's Office will determine the appropriate level of IT Governance maturity required for enabling organizational success.	Closed	As outlined in the audit, the Information Technology Department (ITD) does have citywide governance in place and assigned to staff. This recommendation has been superseded by the ITD Risk Assessment and recommendations within as completed by Baker Tilly in October 2021. This updated assessment extends beyond this identified ITD scope to a broader citywide perspective.
ERP Planning: Data and System Governance	06/13/18	Finding 2: Better citywide data governance will lead to better data in the new ERP system	2.1. Assign roles and responsibilities for data governance (e.g., a "chief data governance officer") to an existing position that reports or could potentially report directly to the City Manager or the Chief Information Officer.	Information Technology	**Concurrence:** Agree **Target date:** July 1, 2019 **Action Plan:** In January 2017, the IT Department hired a qualified data analyst with responsibility for citywide data governance. The role currently reports up through the Chief Information Officer (CIO). The IT Department agrees to request elevation of this role from City Council to a more senior classification to reflect the increased responsibilities expected as a result of implementing an industry- standard data governance framework.	Closed	The ITD continues to have a data analyst position responsible for citywide governance, however, the City has faced significant financial challenges due to the onset of the COVID-19 pandemic and therefore, have significantly reduced staffing resources to manage financial constraints. Therefore, although staff agree this is a best practice and would like to support it, staff no longer agree with the recommendation to reclassify this role to a move senior classification. The financial impacts of this are not the current highest priority for investment in the current reduced resource environment.

Audit Report	Report Date	Finding	Recommendation	Responsible Department(s)	Initial Management Response (upon audit completion)	Current Status As of 9/30/21	Implementation Update As of 9/30/21
ERP Planning: Data and System Governance	06/13/18	Finding 2: Better citywide data governance will lead to better data in the new ERP system	2.2. Adopt an industry standard data governance framework, such as the DAMA-DMBOK, and a process maturity model, such as the COBIT 5 process assessment model. Create a plan to achieve a process capability model of 3 (i.e., “established”) or higher for: • Inventory • Integrity • Migration • Security & Access • Legal Compliance • Availability • Usability	Information Technology	**Concurrence:** Agree **Target date:** December 31, 2019 **Corrective Action:** The IT data lead will work to implement the citywide data strategy that is currently being developed and is part of the FY19-21 IT strategy. Adoption of a standard data governance framework was already identified as a goal in this plan. IT Department agrees to identify and adopt an appropriate, rightsized, industry-recognized, data governance framework. The IT Department working with the City Manager’s Office will determine the appropriate level of data governance maturity required for enabling organizational success.	Closed	The ITD continues to have a data analyst position responsible for citywide governance, however, the City has faced significant financial challenges due to the onset of the COVID-19 pandemic and therefore, have significantly reduced staffing resources to manage financial constraints. Tas identified above, the necessary level of staffing to complete adoption and implementation of a standard data governance framework are not the current highest priority for investment in the current reduced resource environment.
ERP Planning: Separation of Duties	10/17/18	Finding 1: Implementing effective separation of duties and ensuring well-restricted user access controls for the new ERP system will decreasevulnerabilities and risks.	1.a. Transfer the task of entering Accounts Payable invoices to ASD Administration and either discontinue Account Payable’s SAP access for entering invoices or, if not possible, create a procedure that can identify if/when an Accounts Payable invoice is entered by an Accounts Payable employee for supervisory review. 1.b. Have Payroll redesign the existing manual controls to mitigate against the high-risk areas of SoD conflict identified. 1.c. Share with Utilities all relevant SoD practices adopted, and Utilities practices should be consistent with that of ASD.	Administrative Services Department	**Concurrence:** Agree.**Target Date:** With new ERP. **Corrective Action Plan:**1a. Explore the possibility of transferring the task of entering Accounts Payable invoices to ASD Administration.1b. Explore having Payroll redesign the existing manual controls to mitigate against the high-risk areas of SoD conflict identified in the new ERP.1c. Share with Utilities all relevant SoD practices adopted, and Utilities practices should be consistent with that of ASD.	Closed	1a. ASD Administration is responsible for completing invoices specifically for services rendered to the AP team. AP staff continued to park and post all stores invoices, however, before parking inventory must be received in SAP by Stores so there is a third party check. This is a large part of AP’s involvement since discrepancies between the inventory or invoice need to be resolved. It would be inefficient to have non-AP staff perform this review. 1b. AP staff continues to park and post employee reimbursements after receiving approved paperwork from departments. Though not requested, it is expected that requesting departments to park employee reimbursements is inefficient since AP routinely needs to request adjustments after review of the reimbursement paperwork and therefore this would be inefficient. 1a-c. The implementation of a new ERP was cancelled and the City chose to remain on the current ERP platform with SAP. The City has completed a technical upgrade of the current ERP system and is planning a Phase 2 of this upgrade to leverage potential additional tools which is scheduled to be completed in FY 2023 - FY 2024. As part of this phase 2, staff will include this as a desired change, if feasible and cost effective.

Audit Report	Report Date	Finding	Recommendation	Responsible Department(s)	Initial Management Response (upon audit completion)	Current Status As of 9/30/21	Implementation Update As of 9/30/21
ERP Planning: Separation of Duties	10/17/18	Finding 1: Implementing effective separation of duties and ensuring well-restricted user access controls for the new ERP system will decrease vulnerabilities and risks.	2. Information Technology revisit the design and definition of profiles and roles according to the concept of least privilege, where possible.	Information Technology	**Concurrence:** Agree **Target Date:** June 30, 2020 **Corrective Action Plan:** The plan is to review and modify as appropriate the approach to profiles and roles during the design and implementation phases of the new ERP system. If it makes sense timing wise, the new design will be incorporated back into the legacy system during the project. Determination of value and cost in retrofitting to the legacy system will be made during design.	Closed	The implementation of a new ERP was cancelled and the City chose to remain on the current ERP platform with SAP. The City has completed a technical upgrade of the current ERP system and is planning a Phase 2 of this upgrade to leverage potential additional tools which is scheduled to be completed in FY 2023 - FY 2024. As part of this phase 2, staff will evaluate the value and cost in retrofitting the current system as part of the planning for the phase 2 of the system upgrade.
ERP Planning: Data Standardization	10/17/18	Finding 1: Implementing data standardization will ensure increased data accuracy and uniformity in the future ERP system.	1. Provide governance over data standardization, such as who is responsible for data standardization, what data is subject to standardization, what is the data standardization, when does standardization change, etc.	Information Technology	**Concurrence:** Agree **Target Date:** Dec 31, 2019 **Action Plan:** Data standardization and governance are both already priorities of the draft data strategy plan document that is being developed.	Closed	The implementation of a new ERP was cancelled and the City chose to remain on the current ERP platform with SAP. Phase 1 of the upgrade included technical system upgrades and is complete. Phase 2 of the upgrade will consider opportunities for data standardization to the extent feasible. Staff agree that this is best practice, and continue in daily proceedings to make improvements where possible. However, in the absence of the citywide effort to implement a new ERP system and the organization prioritization and additional resources to complete that initiative, this recommendation is no longer relevant.
ERP Planning: Data Standardization	10/17/18	Finding 1: Implementing data standardization will ensure increased data accuracy and uniformity in the future ERP system.	2. Review other systems and implement data standardization, where feasible and beneficial; especially in circumstances when the data feeds into SAP.	Information Technology	**Concurrence:** Agree. **Target Date:** Dec 31, 2019 (For standardization guidance only. Remediation may take significantly longer and will be established once an assessment is made). **Action Plan:** The plan to implement data standardization across systems beyond SAP will be covered in the City's upcoming data strategy plan.	Closed	The implementation of a new ERP was cancelled and the City chose to remain on the current ERP platform with SAP. Phase 1 of the upgrade included technical system upgrades and is complete. Phase 2 of the upgrade will consider opportunities for data standardization to the extent feasible. Staff agree that this is best practice, and continue in daily proceedings to make improvements where possible. However, in the absence of the citywide effort to implement a new ERP system and the organization prioritization and additional resources to complete that initiative, this recommendation is no longer relevant.
ERP Planning: Data Standardization	10/17/18	Finding 1: Implementing data standardization will ensure increased data accuracy and uniformity in the future ERP system.	3. Work with Departments to review the data within SAP and determine what will benefit most by standardizing data.	Information Technology	**Concurrence:** Agree **Target Date:** Dec 31, 2019. **Action Plan:** The plan to identify data and data stewards for SAP to determine standardization benefits will be covered in the City's upcoming data strategy plan.	Closed	The implementation of a new ERP was cancelled and the City chose to remain on the current ERP platform with SAP. Phase 1 of the upgrade included technical system upgrades and is complete. Phase 2 of the upgrade will consider opportunities for data standardization to the extent feasible. Staff agree that this is best practice, however, in the absence of the citywide effort to implement a new ERP system and the organization prioritization and additional

Audit Report	Report Date	Finding	Recommendation	Responsible Department(s)	Initial Management Response (upon audit completion)	Current Status As of 9/30/21	Implementation Update As of 9/30/21
							resources to complete that initiative, this recommendation is no longer relevant.
ERP Planning: Data Standardization	10/17/18	Finding 1: Implementing data standardization will ensure increased data accuracy and uniformity in the future ERP system.	4. Require Departments to implement data standardization requirements during data cleansing in the ERP transition.	Information Technology	**Concurrence:** Agree **Target Date:** Dec 31, 2019. **Action Plan:** This is already a mandatory component of the design phase of implementing the new ERP system.	Closed	The implementation of a new ERP was cancelled and the City chose to remain on the current ERP platform with SAP. Phase 1 of the upgrade included technical system upgrades and is complete. Staff agree that this is best practice, however, in the absence of the citywide effort to implement a new ERP system and the organization prioritization and additional resources to complete data standardization during data cleansing in system transition, this recommendation is no longer relevant.
Code Enforcement Audit	11/06/18	Finding 1: The City resolves many code enforcement cases effectively; but unclear roles and responsibilities, fragmented Municipal Code requirements, and staffing limitations have hampered timely response and resolution	1.1. Clarify and confirm the City's code enforcement strategy and priorities with the City Council. Develop an updated enforcement procedure that is aligned with the confirmed strategy for each area of the City's code enforcement priorities, including case intake, tracking, and reporting. This includes assessment of the regulations that lack an enforcement process or sufficient resources, such as PC district regulations, leaf blower regulations, and conditions of approval requiring the applicant to self-report. Post the updated strategy on the City's code enforcement web page.	CMO	**Concurrence:** Agree **Target Date:** 12 months after item 1.1 and related process redesign is completed. **Action Plan:** The CMO will first coordinate the work of responsible departments on item 1.1 above, and on item 1.2.c to clarify roles and responsibilities in alignment with a revised structure. Once improved practices are clarified, the CMO will work through the CAO and other responsible departments on items 1.2.a, 1.2.b, 1.2.d, and 1.2.e to amend the municipal code as appropriate to improve the administration of code enforcement activities and to align enforcement strategies with organizational responsibilities.	On-Hold	In early 2020 enhancements were made between the City's 311 and Accela software systems providing improved case management, tracking and reporting for staff and end users (more detail provided below). The City's Code Enforcement staffing levels were reduced nearly 70% in FY20/21as a result of the COVID-19 pandemic. In response to fewer resources, staff has prioritized complaints promoting life/safety cases and work without permits. Property maintenance and related complaints are addressed as able. A coordination meeting should be scheduled when resources are available to implement the recommendations and as needed to address critical issues. Recently, in response to property maintenance concerns in neighborhood commercial centers, staff initiated a focused enforcement effort to clean up these sites using one-time funding resources.
Code Enforcement Audit	11/06/18	Finding 1: The City resolves many code enforcement cases effectively; but unclear roles and responsibilities, fragmented Municipal Code requirements, and staffing limitations have hampered timely response and resolution	1.2 Update the Municipal Code sections governing code enforcement, including: a) Combining into a single chapter, clarifying, and streamlining the administrative procedures in PAMC Chapters 1.12 and 1.16 to ensure they support current practices and City Council's intent for code enforcement activities. b) Aligning administrative procedures in other PAMC chapters with the revised administrative procedures	CMO	**Concurrence:** Agree**Target Date:**12 months after item 1.1 and related process redesign is completed.**Action Plan:**The CMO will first coordinate the work of responsible departments on item 1.1 above, and on item 1.2.c to clarify roles and responsibilities in alignment with a revised structure. Once improved practices are clarified, the CMO will work through the CAO and other responsible departments on items 1.2.a, 1.2.b, 1.2.d, and 1.2.e to amend the municipal code as appropriate to improve the administration of code enforcement activities and to align enforcement strategies with organizational responsibilities.	In Progress / On-Hold	As a result of the financial constraints endured due to the onset of the COVID-19 pandemic, there is no longer capacity to focus on these recommended adjustments and they will continue to be on pause until additional resources are restored to this team. The remaining milestones for 1.2 d and e are deferred pending realignment of staff resources from other priorities and supplement department with additional consultant funds or staff resources. *March 2020:* Progress made on items a and b include: On March 2, 2020 Council adopted changes to PAMC 1.12 Administrative Penalties-Citations, to enable

Audit Report	Report Date	Finding	Recommendation	Responsible Department(s)	Initial Management Response (upon audit completion)	Current Status As of 9/30/21	Implementation Update As of 9/30/21
			developed in 1.2.a above as needed and streamlining enforcement activities for consistency across City departments, to the extent possible. c) Clarifying code enforcement roles and responsibilities to ensure they are aligned with the current organizational structure. d) Requiring that permit information and contact information for contractors and responsible City departments be posted at each construction site. e) Removing ambiguities or inconsistencies as part of the annual Municipal Code clean up, including specific position titles, which can change over time.				administrative hearings with partial advance deposit and clarify existing hearing procedures; 2nd reading took place and passed on March 16th, 2020. On February 26, the Planning and Transportation Commission recommended edits to Section 18.01.080 clarifying Title 18 violations can be enforced through processes in Chapter 1.12 and Chapter 1.16 and identifying various enforcement methods to reduce potential confusion about handling zoning code violations and to match charging sections in newly adopted 2019 Building Code updates to Title 16. These changes were approved by Council on March 2, 2020. The revised workplan targets November 2021 for implementation of the remaining milestones in this recommendation.
Code Enforcement Audit	11/06/18	Finding 1: The City resolves many code enforcement cases effectively; but unclear roles and responsibilities, fragmented Municipal Code requirements, and staffing limitations have hampered timely response and resolution	1.3. Hold regular meetings (e.g., quarterly) with staff citywide who have code enforcement responsibilities to share information, discuss resource allocation, and develop collective and consistent enforcement action plans, particularly for where there is overlapping or unclear responsibility.	CMO	**Concurrence:** Agree **Target Date:** Starting 3 months following City Council acceptance of audit report. **Action Plan:** The CMO will convene regular meetings of responsible departments throughout the duration of this corrective action and thereafter routinely convene an interdepartmental working group to monitor and manage the success of the ongoing program.	On-Hold	Upon completion of this audit, an upgrade and evaluation of the 311 system was included as part of the workplan for the City Council's Fiscal Recovery priority in calendar year 2019. However, due to the prioritization of other projects at this time including the work for pursuit of a November 2020 local ballot measure followed by both the onset of the COVID-19 pandemic and vacancies in key positions, this workplan has been placed on hold. Recommendation remains on hold pending predecessor actions.

Audit Report	Report Date	Finding	Recommendation	Responsible Department(s)	Initial Management Response (upon audit completion)	Current Status As of 9/30/21	Implementation Update As of 9/30/21
Code Enforcement Audit	11/06/18	Finding 2: The City does not have complete and reliable code enforcement data to provide useful information for management decisions	2.1. Upon confirming the City's code enforcement strategy and priorities with the City Council in Recommendation 1.1, that the City Manager coordinate with the City's code enforcement functions to: a) Identify what complaint data to capture, track, and share internally and externally. b) Define what constitutes a code enforcement case and identify what case data to capture, track, and share internally and externally. c) Determine which system(s) to use and how to track code enforcement data for each function, including standardizing code enforcement terminology citywide, and design reporting processes capable of aggregating the data into a citywide view. d) Develop performance measures for code enforcement as part of the citywide initiative to improve measures for the annual Performance Report.	CMO	**Concurrence:** Agree **Target Date:** 12-24 months following City Council's acceptance of Recommendation 1.1 **Action Plan:** The CMO will coordinate the work of responsible departments to strengthen citywide data management, including the protection of private and confidential information, related to code enforcement. While performance measures related to code enforcement already exist, considerably improved metrics will be developed (per item 2.1.d) concurrent with the improvement of code enforcement practices throughout this corrective action. Items 2.1.b and 2.1.a are consistent with the priorities of the city's IT Strategic Plan and may be refined iteratively in coordination with item 2.1.c. Estimates may be required for anticipated resource commitments to support new tasks and/or software investments.	On-Hold	This workplan has been placed on hold and therefore delayed as a result of the onset of the COVID-19 pandemic. September 2021 Update: Recommendation remains on-hold pending predecessor actions.

Attachment: OCA - Annual Report (FINAL DRAFT) (13604 : Office of the City Auditor Annual Report)

Audit Report	Report Date	Finding	Recommendation	Responsible Department(s)	Initial Management Response (upon audit completion)	Current Status As of 9/30/21	Implementation Update As of 9/30/21
Code Enforcement Audit	11/06/18	Finding 2: The City does not have complete and reliable code enforcement data to provide useful information for management decisions	2.2 If it is determined under Recommendation 2.1 that Planning will continue to use Accela, Planning should reconfigure Accela Code Enforcement to enhance data collection and reporting, to pave the way for other functions that may adopt Accela, by: a) Defining each type of code enforcement workflow status and identifying additional status or other data points to be captured. b) Working with the Accela consultant to ensure needed data and documents are captured accurately, consistently, and in a manner that can be extracted for reporting. This may include:· Adding new workflow status and creating additional data fields to capture new data points.· Adding or modifying drop- down lists.· Allowing certain data fields to be modified after initial data entry. c) Developing report templates in Accela for periodic reporting of code enforcement performance measures developed in Recommendation 2.1.d. d) Establishing data entry procedures to prevent errors and improve consistency. This may include:· Establishing naming conventions for attachments.· Ensuring that information displayed on BuildingEye provides sufficient detail for the public to understand the issue, status, and resolution of each case.	CMO	**Concurrence:** Agree**Target Date:** Concurrent with item 2.1; 12-24 months following City Council's acceptance of Recommendation 1.1 **Action Plan:**The CMO will coordinate the work of Planning and other responsible departments to integrate data collection and reporting functions into the appropriate data management system.	On-Hold	This workplan has been placed on hold and therefore delayed as a result of the onset of the COVID-19 pandemic. The revised workplan targets November 2020 - November 2022 for the remaining implementation milestones. *March 2020:* The "311" Customer Relationship Management (CRM) system for Code Enforcement required integration of 311 CRM and Accela systems to prevent duplication of effort and potential tracking oversights for both the community and City CEOs. Integration began late 2018 and was impacted by Accela mergers and acquisitions of other companies leading to Accela's shifting priorities and changes in its organizational structure. CEOs were required to monitor both systems and adopted an 'interim' process to help minimize issues caused by having two systems/databases for code cases. Progress in the 3rd quarter 2019 with Accela's new project manager furthered the integration (e.g., a firm timeline and allocation of well-defined tasks and requirements for all parties). February 2020 began integration in the Accela 'test' environment, with a demonstration on both systems on 03/03/20. City staff are satisfied with the specifications and behavior. The integration will allow community members to continue to submit real-time issues or 'service requests' via 311 CRM while eliminating the duplication of records between the two systems. Improvements included new workflows with more specificity on the code issue, and new drop downs with new selections. The Accela merger enabled the info pushed to Building Eye to provide detail allowing public understanding of the issue, the status, and when each case is resolved. Staff is still working on the capability to modify fields after initial data entry, and specific naming conventions for attachments. Preparations for launching into 'production' are underway. The City expects to complete and 'launch' the integrated system by April of 2020.

Attachment: OCA - Annual Report (FINAL DRAFT) (13604 : Office of the City Auditor Annual Report)

Audit Report	Report Date	Finding	Recommendation	Responsible Department(s)	Initial Management Response (upon audit completion)	Current Status As of 9/30/21	Implementation Update As of 9/30/21
Code Enforcement Audit	11/06/18	Finding 3: The City actively engages with individuals responsible for code violations to gain compliance but should improve its public communication on code requirements and enforcement efforts	3.1 Provide general, citywide information on code enforcement in a central location on the City's website and assign responsibility for ensuring that the information is kept up to date. Examples of information that the website should include are: a) The City's code enforcement strategy and priorities (see Recommendation 1.1). b) Enforcement process, administrative procedures, and penalties (see Recommendations 1.2.a and 1.2.b). c) A list of common code enforcement issue types with a brief description of code requirements, how to report a violation, and contact information for the responsible City function and/or link to additional information on the function's website (see Recommendation 1.2.c). d) How to track code enforcement case status and resolution, including links to BuildingEye, the City of Palo Alto Citizen Portal, or PaloAlto311. e) General information on how a complaint is managed, including what level of communications and information the complainant can expect and examples of information that the complainant is not entitled to receive, if any. f) City programs, community partners, and other neighborhood resources available to provide assistance.	CMO	**Concurrence:** Agree **Target Date:** 3 months following implementation of Recommendation 2.2 **Action Plan:** The CMO will coordinate the work of responsible departments to implement code enforcement strategies and priorities.	On-Hold	This workplan has been placed on hold and therefore delayed as a result of the onset of the COVID-19 pandemic. Recommendation remains on hold pending predecessor actions. *March 2020* The City website features a page for "Common Code Concerns & Contacts." It clarifies which issues fall under the purview of Planning, Public Works, Police, or outside agencies with phone numbers and links to their respective webpages for more information. It also links to the PaloAlto311 information. It was most recently updated *February 6, 2020.* As the casework intake and tracking system is improved through the implementation of the workplan related to other recommendations in this report, the website will be updated accordingly. This workplan is also being integrated with the City's new website redesign.

Audit Report	Report Date	Finding	Recommendation	Responsible Department(s)	Initial Management Response (upon audit completion)	Current Status As of 9/30/21	Implementation Update As of 9/30/21
Code Enforcement Audit	11/06/18	Finding 3: The City actively engages with individuals responsible for code violations to gain compliance but should improve its public communication on code requirements and enforcement efforts	3.2. Assign staff to be responsible for citywide administration of PaloAlto311 to provide ongoing maintenance and support in coordination with code enforcement functions across the City, including: a) Redefining PaloAlto311 issue types and reconfiguring workflows to provide clearer options for complainants who are reporting issues and to minimize incorrect routing of service requests. b) Managing user access and making training materials available for new users. c) Updating and maintaining the PaloAlto311 data and dashboard on the City's Open Data Portal.	CMO	**Concurrence:** Agree **Target Date:** Concurrent with recommendation 2.2 (12- 24 months following City Council's acceptance of Recommendation 1.1) **Corrective Action Plan:** The CMO will coordinate the work of responsible departments on administration of citywide code enforcement efforts.	On-Hold	This workplan has been placed on pause and therefore delayed as a result of the onset of the COVID-19 pandemic. Recommendation remains deferred pending predecessor actions. *March 2020* Revised workplan targets November 2020 - November 2022 for implementation milestones.
Audit of Nonprofit Service Agreements	08/29/19	The Office of Human Services effectively monitors contractor performance using an established process and tools, which can help other City departments better administer their nonprofit service agreements.	Work with the Administrative Services Department's Purchasing Division, the City Attorney's Office, and the Community Services Department's Office of Human Services to create a citywide template for nonprofit service agreements, and make it available to all City departments. The template should ensure that the City's payments are tied to contractor performance by: a) Specifying program goals, measurable objectives, and performance targets are specified in the scope of services. b) Requiring specific deliverables (e.g., semiannual report, financial statements) are submitted along with each invoice, rather than requiring "a detailed statement" in broad terms that could besubject to interpretation. c) Requiring all deliverables be provided prior to the final payment.	ASD/CAO/CSD/CMO	**Concurrence:** Agree **Target Date:** December 2020 **Action Plan:** Sept 2019 – June 2020:Interdepartmental team reviews and makes adjustments to business processes for nonprofit service agreement creation and management. June 2020 – December 2020: Develop template(s) and any other necessary implementation materials or guidelines.	Closed	Current practice of staff is to evaluate new partnerships arise, staff have been working to ensure coordination and clear agreements while balancing the unique relationships each partner may have. When appropriate, as identified in this audit for like programs such as the award of Human Services Resource Allocation Process (HSRAP), staff does use similar agreements. In the absence of a template, staff routinely coordinate internally by impacted parties and review prior agreements for like terms and consistency.

Attachment: OCA - Annual Report (FINAL DRAFT) (13604 : Office of the City Auditor Annual Report)

Audit Report	Report Date	Finding	Recommendation	Responsible Department(s)	Initial Management Response (upon audit completion)	Current Status As of 9/30/21	Implementation Update As of 9/30/21
Audit of Nonprofit Service Agreements	08/29/19	The Office of Human Services effectively monitors contractor performance using an established process and tools, which can help other City departments better administer their nonprofit service agreements.	2. Renew the 2004 agreement with PADBPA to: a) Require that a preliminary BID budget be submitted in accordance with the City's budget schedule to ensure that the City operating budget is aligned with the PADBPA's budget. b) Require that PADBPA include in its annual report previous two years' budgeted and actual revenues and expenses in a format similar to the City's operating budgets for better projection of the following fiscal year budget. c) Require that collection status, including delinquencies and any subsequent collections by PADBPA, be included in the annual report. d) Reflect the outsourcing of the assessment invoicing and collection and elimination of the Economic Development Manager position.	CMO/CAO/ASD	**Concurrence:** Agree **Target Date:** June 2020 **Action Plan:** Sept – Dec 2019: Partner with PADBPA to identify shared understanding of agreement requirements. Jan – June 2020: Partner with CAO and PADBPA to propose revised agreement language and renewal of the agreement to City Council.	On-Hold	As a result of the onset of the COVID-19 pandemic, and the City Council's action to place any assessment of the Downtown Business Improvement District (BID) on hold, operations of the Downtown BID, including relationships with PADBPA have been placed on hold. The City Council has waived the BID assessment fee through FY 2022. Staff anticipate that in planning for FY 2023 over the coming fiscal year, that staff will work with PADBPA or its successor to incorporate the recommendations into the ongoing partnership. The assessment invoicing and collection associated with the BID is now the responsibility of MuniServices to coincide with the BRC invoicing and system for ease of the businesses. **Expected Completion Date:** FY 2023 Q1
Audit of Nonprofit Service Agreements	08/29/19	The Office of Human Services effectively monitors contractor performance using an established process and tools, which can help other City departments better administer their nonprofit service agreements.	3. Establish a procedure or desk manual to clarify roles and responsibilities for monitoring the BID Fund records in SAP, PADBPA's financial records, and MuniServices' assessment collection data to ensure that accurate and complete financial data are provided to the City Council for informed budget and funding decisions.	CMO	**Concurrence:** Agree **Target Date:** March 2020 **Action Plan:** Incorporate into workplan for item 2.	On Hold	As a result of the onset of the COVID-19 pandemic, and the City Council's action to place any assessment of the Downtown Business Improvement District (BID) on hold, operations of the Downtown BID, including relationships with PADBPA have been placed on hold. The City Council has waived the BID assessment fee through FY 2022. Staff anticipate that in planning for FY 2023 over the coming fiscal year, that staff will work with PADBPA or its successor to incorporate the recommendations into the ongoing partnership. Internally, the Administrative Services Department has assumed responsibility of the financial responsibilities of the BID Fund with the transfer of the BRC from DSD to ASD as well. The management of the PADBPA contract remains with the CMO. The assessment invoicing and collection associated with the BID is now the responsibility

Audit Report	Report Date	Finding	Recommendation	Responsible Department(s)	Initial Management Response (upon audit completion)	Current Status As of 9/30/21	Implementation Update As of 9/30/21
							of MuniServices to coincide with the BRC invoicing and system for ease of the businesses. **Expected Completion Date:** FY 2022 Q4
Audit of Nonprofit Service Agreements	08/29/19	The Office of Human Services effectively monitors contractor performance using an established process and tools, which can help other City departments better administer their nonprofit service agreements.	4. Establish an overall monitoring method to ensure that nonprofit organizations with multiple agreements with the City are reviewed by all responsible departments to avoid redundancy while clarifying the goals, objectives, and performance measures to be tracked under each agreement.	ASD	**Concurrence:** Agree **Target Date:** June 2020 **Action Plan:** Identity required resources including staff support to complete this function, develop a proposal for implementation to be considered as part of the annual budget process.	Closed	Baker Tilly is currently in process of a non-profit agreement audit. During that effort Baker Tilly will follow-up on outstanding audit recommendations and account for them in their current audit activity.