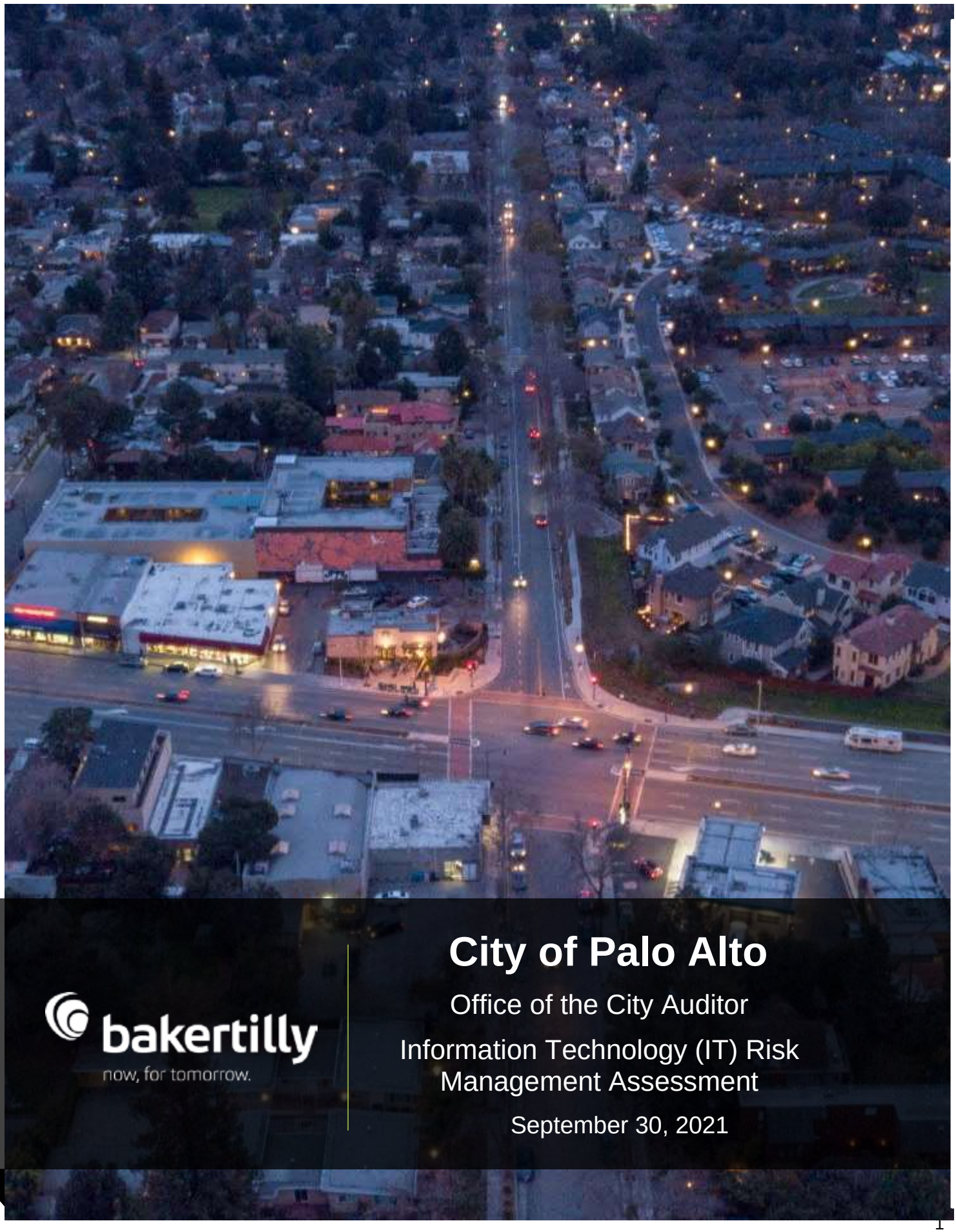

City of Palo Alto

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.

Table of Contents

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.

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:

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.

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**

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**

Palo Alto IT Risk Management Assessment
Appendix A: Risk Matrix

bakertilly

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**

Palo Alto IT Risk Management Assessment
Appendix A: Risk Matrix

bakertilly

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**

Palo Alto IT Risk Management Assessment
Appendix A: Risk Matrix

bakertilly

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**

Palo Alto IT Risk Management Assessment
Appendix A: Risk Matrix

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**

Palo Alto IT Risk Management Assessment
Appendix A: Risk Matrix

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**

Palo Alto IT Risk Management Assessment
Appendix A: Risk Matrix

bakertilly

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**

Palo Alto IT Risk Management Assessment
Appendix A: Risk Matrix

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**

Palo Alto IT Risk Management Assessment
Appendix A: Risk Matrix

bakertilly

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**

Palo Alto IT Risk Management Assessment
Appendix A: Risk Matrix

bakertilly

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**

Palo Alto IT Risk Management Assessment
Appendix A: Risk Matrix

bakertilly

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

bakertilly

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**

Palo Alto IT Risk Management Assessment
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-

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.

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.

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

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.