August 1, 2024

City of Palo Alto

Office of City Auditor

Parking Permit Technology Contracts Audit

Contents

Executive Summary

Purpose of the Audit

Baker Tilly US, LLP (Baker Tilly), in its capacity serving as the Office of the City Auditor (OCA) for the City of Palo Alto (the City), conducted an audit of the parking permit technology systems contract management process and controls based on the approved Task Order 4.16. The objectives of this review were to:

1) Determine whether adequate policies and procedures are implemented effectively to protect the privacy of personal information gathered using parking permit technology for the City's parking management.
2) Determine whether the City monitors the vendor's performance to ensure compliance with contract terms and applicable laws and regulations related to data privacy.

Report Highlights

Finding 1: **Data Privacy Improvements**

The City lacks a data privacy program owner and policies, procedures and associated training requirements have not been regularly updated.

Key Recommendation

We recommend the City designate a data privacy program owner to coordinate a uniform approach to data privacy management between the City Attorney, Chief Information Officer, and Director of Human Resources.

Finding 2: **Lack of Personal Identifiable Information (PII) Procedures**

The City does not have Personal Identifiable Information (PII) procedures for personal information that is managed or collected. Additionally, there are no procedures related to masked or de-identified personal information.

Key Recommendation

We recommend that the City establish procedures for managing and collecting Personal Identifiable Information (PII). These procedures should include: classification of information, retention of PII, access control, data masking, and data restoration and backup.

Finding 3: **Records and Information Management Policy Enhancements**

The City's Records and Information Management Policy does not address essential elements related to information collection consent, management protocols for personally identifiable information (PII), and comprehensive guidelines governing data retention, maintenance, and destruction.

Key Recommendation

We recommend the City should annually review and approve its Records and Information Management Policy to ensure it aligns with best practices and relevant laws.

Finding 3: **Lack of User Access Listing and Reviews**

The City could not provide a user access listing for individuals who have access to Personal Identifiable Information (PII) and there are no individuals that are considered data security owners. Additionally, there is no evidence that access reviews are being performed periodically by data security owners and confirmed with the IT Department.

Key Recommendation

We recommend that the City establishes a list of individuals who have access to add, edit, or delete Personal Identifiable Information (PII).

Finding 4: **Inadequate Breach of Contract Terms and Conditions with Third-Party Vendor**

There is a section called "Data Security Breach Notification Act" within the City's Data Privacy Policy, however, there is no specific mention of breaches related to third-party vendors.

Key Recommendation

We recommend that the City's Data Privacy Policy explicitly covers breaches that occur to third-party vendors. The policy should specifically emphasize that vendors are required to adhere to and uphold the data privacy and security standards set by the City.

Finding 5: **Inadequate Vendor Performance Assessment**

There is no formal vendor performance assessment in place within the Transportation Department.

Key Recommendation

We recommend that the Transportation Department establishes a formal vendor performance assessment for all third-party vendors.

Finding 6: **Absence of Third-Party Agreement Requirements**

The City’s third-party license plate reading provider agreement does not formally define the minimum requirements and vendor expectations related to the workflows that process PII data.

Key Recommendation

The City should implement internal controls to ensure that all third-party providers and agreements are in alignment with Palo Alto's maximum risk appetite and risk posture.

Introduction

Objective

The objectives of this review were to:

1) Determine whether adequate policies and procedures are implemented effectively to protect the privacy of personal information gathered using PARKING PERMIT technology for the City's parking management.
2) Determine whether the City monitors the vendor's performance to ensure compliance with contract terms and applicable laws and regulations related to data privacy.

Background

During the FY2022 risk assessment, the Baker Tilly team identified the following inherent risks and noted the contract management as a high-risk area:

- Contract compliance and cost control issues
- Noncompliance with applicable data privacy laws

The summary of the information provided in the FY2022 operating and capital budget documents prepared by the City of Palo Alto (the City) is as follows:

Budget Summary

	FY 2019 Actuals	FY 2020 Actuals	FY 2021 Adopted Budget	FY 2022 Adopted Budget	FY 2022 Change $	FY 2022 Change %
Dollars by Division						
Administration	$473,466	$546,829	$630,126	$660,887	$30,762	4.9%
Engineering and Planning	$499,205	$604,794	$604,400	$618,138	$13,738	2.3%
Programs	$861,232	$900,441	$669,648	$468,065	$(201,583)	(30.1)%
Total	**$1,833,902**	**$2,052,064**	**$1,904,173**	**$1,747,089**	**$(157,084)**	**(8.2)%**
Salary & Benefits						
Healthcare	$50,920	$68,462	$103,177	$81,839	$(21,338)	(20.7)%
Other Benefits	$11,358	$20,569	$26,528	$28,610	$2,082	7.8%
Overtime	$2,897	$1,439	$7,795	$7,998	$203	2.6%
Pension	$116,288	$264,762	$304,620	$334,724	$30,104	9.9%
Retiree Medical	$74,971	$77,220	$78,098	$89,159	$11,061	14.2%
Salary	$431,343	$662,149	$791,163	$721,229	$(69,934)	(8.8)%
Workers' Compensation	$15,948	$24,355	$21,922	$32,800	$10,878	49.6%
Total Salary and Benefits	**$703,726**	**$1,118,955**	**$1,333,304**	**$1,296,359**	**$(36,944)**	**(2.8)%**
Dollars by Category						
Allocated Charges	$133,778	$152,710	$184,424	$204,334	$19,910	10.8%
Contract Services	$754,971	$558,029	$132,446	$41,800	$(90,646)	(68.4)%
Facilities & Equipment	–	$945	$5,000	$5,000	–	–%
General Expense	$233,380	$218,077	$228,750	$189,346	$(39,404)	(17.2)%
Operating Transfers Out	$7,780	–	–	–	–	–%
Supplies & Material	$267	$3,347	$20,250	$10,250	$(10,000)	(49.4)%
Total Dollars by Expense Category	**$1,833,902**	**$2,052,064**	**$1,904,173**	**$1,747,089**	**$(157,084)**	**(8.2)%**
Revenues						
Operating Transfers-In	$128,000	$128,000	$128,000	$128,000	–	–%
Other Revenue	–	$12,000	–	$60,000	$60,000	–%
Permits and Licenses	$13,332	$37,919	$13,332	$13,332	$0	–%
Total Revenues	**$141,332**	**$177,919**	**$141,332**	**$201,332**	**$60,000**	**42.5%**
Positions by Division						
Administration	0.50	2.18	2.33	1.75	(0.58)	(24.9)%
Engineering and Planning	2.18	1.70	1.70	1.90	0.20	11.8%
Programs	2.21	2.80	2.80	1.55	(1.25)	(44.6)%
Total	**4.89**	**6.68**	**6.83**	**5.20**	**(1.63)**	**(23.9)%**

Systems Involved

- Permitting System, City of Palo Alto
- Processing System, Duncan Solutions
- Automated License Plate Reader, ComSonics

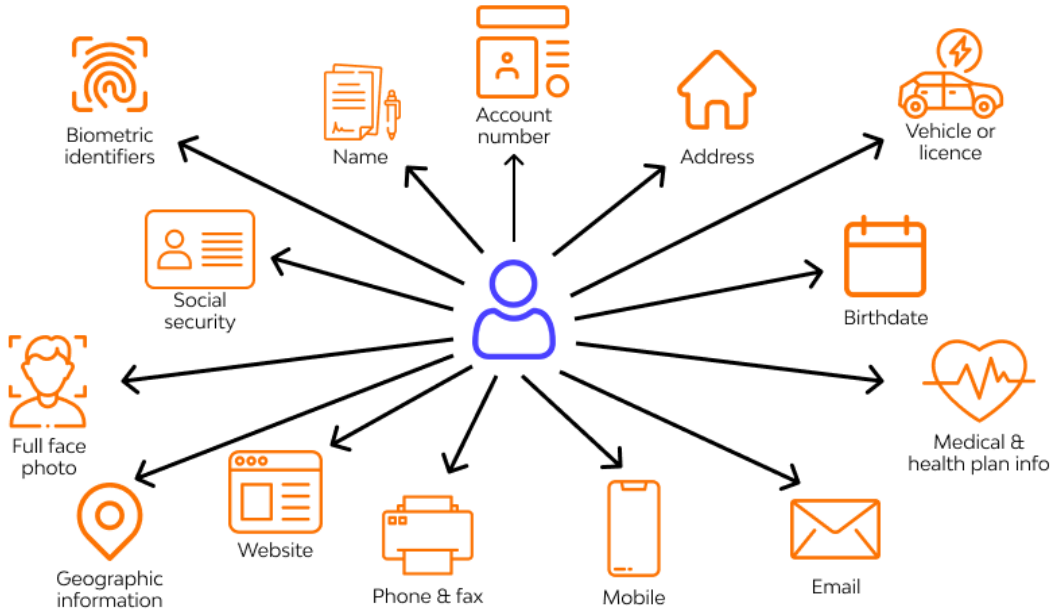
Risk Consideration

Based on the currently available information, we have identified the following risks associated with management of the Office of Transportation:

- Data Privacy
- Contract Management
- Safety Improvement Projects
- Traffic Operations

Personally Identifiable Information (PII)

According to the National Institute of Standards and Technology (NIST), the definition of personally identifiable information (PII) is: "Information that can be used to distinguish or trace an individual's identity—such as name, social security number, biometric data records—either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.)."



It is crucial for the City to define their posture as it relates to data privacy and PII because this will allow the City to ensure that all providers are complying with the City's standards.

Data Security Owner

Each data security owner (the City, Duncan Solutions, and ComSonics) is responsible for the classification, protection, storage, use, and quality of data processed related to parking permitting and enforcement operations.

Data Life Cycle

At a high level, the data life cycle involves the suggested steps below, followed by Palo Alto's current, related practices:

1. Data Collection:

   Data should be gathered in standardized formats, so it can be accessible and manageable later in the cycle.

   - Palo Alto customers apply for permits online, which includes PII and PCI.

2. Data Storage

   Policies should be established related to the storage of data.

   - Data is stored in the City's permitting system, Duncan Solutions'

processing system, and the ComSonics system.

3. Data Maintenance

   Data should be made usable and available for the appropriate person(s).

   - Palo Alto's customer application data is used to generate permits.

4. Data Usage

   Data is used for making decisions.

   - Verification of active permits is performed by scanning license plate numbers into the parking permit system and validating against Duncan Solutions' processing system, which pulls from the City's permitting system.

5. Data Cleaning

   When data is no longer useful, data should be deleted, purged, destroyed, or archived.

   - Palo Alto customers permits that are inactive or expired should be purged based on the City's records retention schedule.

Scope

The scope of this audit was to review the parking permit technology systems contract management. The OCA reviewed the City of Palo Alto's policies and procedures related to Privacy Management, Data Management and Collection, Data Security, 3rd Party C&C Agreements, Surveillance Policy, and Incident Management in relation to the use of the parking permit technology and to ensure that the City maintains all necessary policies and that they are up to date. In addition to the policies and procedures, the OCA reviewed the City's vendor performance monitoring.

Methodology

1. In order to address our audit objective (1), we performed the following procedures:
   - Interviewed the appropriate individuals to understand the process, the information system used, and internal controls related to the gathering of personal information collected by the parking permit technology systems.
   - Reviewed the contracts, policies, and procedures as well as the regulations and standards to identify the criteria to be used for evaluation of compliance and control design and effectiveness.
   - Reviewed the documents (such as contracts and supporting documents for allocation) for selected samples.
   - Compared privacy control against the California Consumer Privacy Act of 2018 and other best practices.
2. In order to address our audit objective (2), we performed the following procedures:
   - Interviewed the appropriate individuals to understand the process and internal controls over compliance with contracts, regulations, and vendor monitoring.
   - Reviewed agreements between Palo Alto and Duncan Solutions to identify compliance requirements.
   - Identified the monitoring activities performed by management to ensure the compliance.
   - Reviewed the relevant documents to evaluate the effectiveness of compliance monitoring activities.

Compliance Statement

This audit activity was conducted from February 2023 to December 2023 in accordance with generally accepted government auditing standards, except for the requirement of an external peer review[1]. 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.

Organizational Strengths

During this audit activity, we observed certain strengths of the City. Key strengths include:

- Transportation Department was responsive and helpful.
- All involved departments provided responses to all requested items.
- Knowledge and expertise of third-party providers.

[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 with Baker Tilly U.S, LLP for internal audit services for October 2020 through June 2022 with an extension through June 2025. City Council appointed Kate Murdock, Audit Manager in Baker Tilly's Risk Advisory practice, as City Auditor in May 2024. As a result of transitions in the Audit Office and peer review delays due to the COVID pandemic, an external peer review is targeted for 2025. It should be noted that Baker Tilly's most recent firmwide peer review was completed in October 2021 with a rating of "Pass". The scope of that peer review includes projects completed under government auditing standards. A report on the next firmwide peer review should be available later in 2024.

The Office of the City Auditor greatly appreciates the support of the Information Technology, Human Resources, and Transportation Departments in conducting this audit activity.

Thank you!

Detailed Analysis

Policies and Procedures

The City has the Data Privacy Policy (Revised: April 2019). The Policy Statement of this policy is "this Data Privacy Policy describes the data privacy requirements and procedures for the protection of personal data and personal information of individuals (the "Data") created, collected, processed, received, stored, and transmitted by the City of Palo Alto (the "City")."

The City's Data Privacy Policy includes User Data Collected, Stored, Processed, and Shared; Information Security and Data Protection; Data Security Breach Notification Act; Third-Party Data Access Control; Information Disclosure; California Privacy Rights; Protecting Children's Privacy Online; and City of Palo Alto Utilities ("CPAU") Data Privacy. The policy does not include the following related best practices:

- Guidance on the measures in place to secure and protect PII from unauthorized access, disclosure, alteration, and destruction. This may include encryption, access controls, and regular security audits.[2]
- A clear definition of Data Subject Rights that outlines the rights of individuals regarding their personal information[3].

The City has the Records and Information Management Policy (Revised: July 2000). The policy statement of this policy is that it "was developed to ensure the efficient retention and protection of information and to assure the availability of information to the public in accordance with the State of California Public Records Act."

The City's Records and Information Management Policy includes Roles and Responsibilities and a Compliance Requirements section. The policy does not include the following related best practices[4]:

- A formal definition of record categories or types of data that guides how data is retained.
- A procedure for destroying or disposing of records once they have reached the end of their retention period.
- A procedure for exceptions and legal holds as records may be exempt from regular retention periods.
- Guidance on individuals that have access to the various types of records.
- Guidance on any training programs or awareness campaigns that are related to record retention.
- Guidance on the monitoring of record retention activity and consequences of non-compliance.

There is also a Data Retention Schedule that supplements the Records and Information Management Policy. The retention schedule identifies which records are permanently retained as well as department-specific retention of records.

[2] California Consumer Privacy Act of 2018, Section 1798.185 - Codes Display Text (ca.gov)
[3] Chapter 3 – Rights of the data subject - General Data Protection Regulation (GDPR) (gdpr-info.eu)
[4] A complete guide to business Records Retention | Iron Mountain United States

Best Practices

As organizations and businesses move online and communicate digitally, the risk of data breaches and/or private information leaks are higher than ever. Personally identifiable information (PII) can be used for targeted attacks, social engineering attacks, identity theft, and more. Effective and updated policies and procedures are integral to protecting the City from breaches of PII. Through researching standards related to PII, data privacy, and records management & retention, the OCA compiled the following list of best practices according to the California Consumer Privacy Act (CCPA), the Information Systems Audit and Control Association (ISACA), and National Institute of Standards and Technology (NIST).

- Educate and train employees on a consistent basis on topics related to PII, data privacy, security, incident management, and cybersecurity.
- Obtain explicit and informed consent from individuals before collecting their personal information.
- The purposes for which personal data are collected should be specified at the time of data collection.
- Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.
- Conduct periodic data audits and/or risk assessments to identify vulnerabilities, compliance gaps, and areas for improvement.
- Review policies and procedures on an annual basis to ensure accuracy and that all information is up to date.
- Ensure that all policies and procedures related to PII, data privacy, and security are available for City employees and external users.

The vendor contract owner should be responsible for all quantitative and qualitative key performance indicator identification, monitoring and reporting to Executive Leadership related to but not limited to the following:

- Quality - error resolution
- Delivery - availability
- Innovation - proposed improvements
- Risk - breaches and non-compliance
- Cost - price increase and scope limitations
- Customer Service - compliant resolution and communication

Audit Results

Finding 1: Data Privacy Improvements

The City lacks an identified citywide data privacy program owner and policies, procedures and associated training requirements have not been updated recently.

Recommendation

We recommend the City designate a data privacy program owner to coordinate a uniform approach to data privacy management among the City Attorney, Chief Information Officer and Director of Human Resources. Based on best practices, the data privacy program owner responsibilities should include the following:

- Annual review and update of data privacy policies and procedures in alignment with the California Consumer Privacy Act of 2018. Reviews should be appropriately documented.
- Annual data privacy trainings held with all departments. The City might also consider use of a Certified Information Privacy Professional (CIPP) to ensure compliance with data privacy laws, regulations, and best practices. Training compliance should be tracked and monitored, and metrics might include: completion rate, assessment scores, feedback, and survey responses, and reported to management quarterly. Every employee is expected to take privacy management training.
- Ensure data privacy requirements and changes are annually incorporated into the City's Record and Information Retention Policy so records containing personal identifiable information are properly secured. Additionally, documented procedures for data destruction should be aligned with legal requirements,

Management Response

Responsible Department(s): Information Technology

Concurrence: Agree

Target Date: CY Q4 2024

Action Plan: While the City Does not have a designated data privacy program owner, the Data Privacy Policy provides oversight for the shared responsibility amongst the roles and departments, though staff agree the policy review and updates. A project to update all IT policies has been initiated and this policy will be reviewed as part of this project, specifically in alignment with NIST regulations. This initiative has been started in alignment with the Cybersecurity Audit that recommended review of Outdated Policy and Standards Documentation recently completed in FY 2023. Although cybersecurity training is already offered and required citywide, to provide privacy training opportunities, a newly procured security training platform will provide training related to data protection, compliance with privacy laws and regulations, and best practices related to data privacy.

Finding 2: Lack of Personal Identifiable

The City does not have specific Personal Identifiable Information (PII) procedures for personal information that is managed or collected in

Information (PII) Procedures	the parking permit systems. In addition, there are no procedures or guidelines regarding if or which information should be de-identified to protect information privacy.
Recommendation	We recommend when implementing a system such as the parking permit systems, that the City documents procedures related to Personal Identifiable Information (PII) when managing or collecting personal data in that system. Procedures for PII data should include how to classify sensitive and non-sensitive information, which PII is necessary for retention, access control, data masking (what type of data is redacted or even replaced), contract terms to manage vendor relationships where PII is referenced or shared, and data that is restored or backed up. Once established the procedures should be easily accessible to program staff.
Management Response	**Responsible Department(s):** Information Technology **Concurrence:** Partially Agree **Target Date:** CY Q4 2024 **Action Plan:** Procedures on handling PII are included and maintained as part of Information Privacy policy provided for review. In addition, a Surveillance Policy is also maintained and reported on annually for new technologies implemented prospectively. Specifically, parking permit data is limited to parking permit program and collections staffing. More specificity regarding PII handling can be added and identified in these policies already under review.
Finding 3: Lack of User Access Listing and Reviews	The City did not provide a user access listing for individuals who have access to Personal Identifiable Information (PII) for the parking permit systems and no designation of the data security owner(s). Additionally, there is no evidence that access reviews are being performed periodically.
Recommendation	We recommend that the City establishes a list of individuals who have access to add, edit, or delete Personal Identifiable Information (PII). The City should review user access rights annually by the identified data security owners in departments.
Management Response	**Responsible Department(s):** Information Technology **Concurrence:** Agree **Target Date:** CY Q4 2024 **Action Plan:** Vendors required to supply role-based access control to managed user access levels and those permissions/restrictions are established upon user set-up. Staff will evaluate updates to centralized process requirements in the review of data privacy policy and procedures including feasibility to develop reports will be shared with the appropriate staff to validate only authorized staff have access to PII across many software platforms.

Finding 4: Inadequate Breach of Contract with Third-Party Vendor	There is a section called "Data Security Breach Notification Act" within the City's Data Privacy Policy, however, there is no specific mention of breaches related to third-party vendors.
Recommendation	We recommend that the City's Data Privacy Policy explicitly covers breaches that occur to third-party vendors. The policy should specifically emphasize that vendors are required to adhere to and uphold the data privacy and security standards set by the City. Additionally, the policy should specify that third-party vendors must follow the City's data classifications and requirements. The City's data breach response plan should identify a key point of contact, defined approved communication methods, the maximum timeframe for which the incident should be communicated to the City, and the minimum requirements for key information that should be provided.
Management Response	**Responsible Department(s):** Information Technology **Concurrence:** Partially Agree **Target Date:** CY Q4 2024 **Action Plan:** All vendors are required to agree to the City's Cybersecurity Terms and Conditions which requires notification of a security breach, this is evidenced by the ALPR contract approved in 2021 which included these terms. Specific updates to specify a response plan expectations in the policy will be reviewed as part of the project to update all IT policies as staff agreed the policy is in need of review and update.
Finding 5: Inadequate Vendor Performance Assessment	The City does not have a formal process to ensure on-going vendor compliance with the Vendor Information Security Assessment (VISA) Questionnaire through the full term of the parking permit systems contracts.
Recommendation	We recommend that the Transportation Department establish a formal vendor performance assessment for all third-party vendors. This assessment would help evaluate potential risks, identify benefits of working with a vendor, and confirm that the vendor is fulfilling the terms of the contract while delivering value in the relationship. Specific tests that can be performed during a third-party assessment are performance tests, delivery tests, customer service tests, cybersecurity tests, and compliance tests.
Management Response	**Responsible Department(s):** Information Technology, Office or Transportation, Administrative Services **Concurrence:** Partially Agree **Target Date:** Q4 CY 2024 **Action Plan:**

The Office of Transportation is responsible for contract management and has an informal process to ensure service providers are meeting scope of services described within. A more formal process to ensure continued compliance with cyber security requirements through the term of the contract will be reviewed among Administrative Services, Office of Transportation, and Information Technology to determine an appropriate procedure. Staff is reviewing this in alignment with the IT risk management process which was recommended as part of the Risk Management Assessment completed by Baker Tilly previously.

Finding 6: Absence of Third-Party Agreement Requirements

The City's third-party license plate reading provider agreement does not formally define the minimum requirements and vendor expectations related to the workflows that process PII data.

Recommendation

The City should implement internal controls to ensure that all third-party providers and agreements are in alignment with the Palo Alto's maximum risk appetite and risk posture in the following areas:

- Contractual language for the management of that have access to City PII data.
- Duly executed contracts are in place with third parties managing or that have access to workflows related to PII data.
- Third-party companies responsible for or that have access to workflows which are related to PII are appropriately risk ranked in order to assess exposure to privacy data leakage.
- Self-assessment of third-party vendors is managed and reviewed to ensure performance is satisfactory.

Management Response

Responsible Department(s): Information Technology & Administrative Services

Concurrence: Partially Agree

Target Date: Q4 CY 2024

Action Plan:

The City currently has a procurement process that involves the requesting department, legal review, and consultation with stakeholders such as Information Technology or Human Resources. This process will be detailed in the nearly completed Procurement Audit. Standard contract templates that are in alignment with the City's risk tolerance levels are used when possible, when changes or alternative contract documents are necessary they are reviewed by these parties in depth to ensure general compliance with risk exposure. As such, this continues to be a living process as both service providers and industry standard practices evolve; staff agree that as more technology contracts are required for the delivery of services, clarity in risk tolerance and alignment with contract terms will continue to be adjusted.