City of Phoenix

Citywide
Privacy Program

July 17, 2024

Mission Statement

To improve the quality of life in Phoenix through efficient delivery of outstanding public services.

Report Highlights

Privacy Program Governance

The City has made progress identifying weaknesses in the privacy program and is actively working to resolve them.

Risk Management Strategy

Information Management Plans (IMP) have not been maintained as required by City policy.

Awareness and Training

The City does not have a stand-alone privacy awareness training course.

Project Team

Aaron Cook
City Auditor

Stacey Linch
Deputy City Auditor

Mahdi Lasker
Sr. Internal Auditor - IT

Project Number

1240043

This report can be made available in alternate format upon request.

City Auditor Department
140 N 3rd Avenue Phoenix, AZ 85003
602-262-6641 (TTY use 7-1-1)

Executive Summary

Purpose

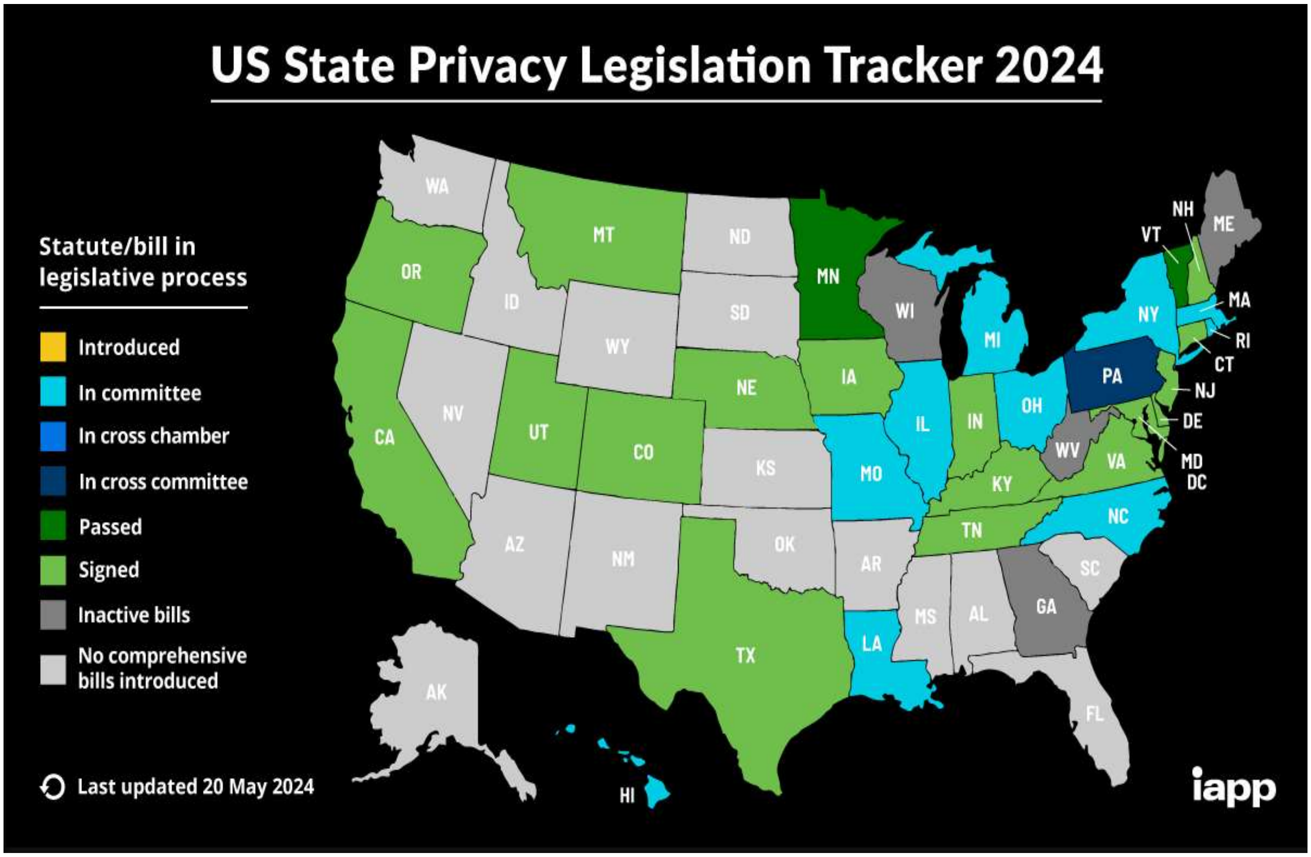
Our purpose was to assess the governance of the Privacy Program to validate compliance with City policies and Arizona Revised Statues (A.R.S.), and alignment with industry standards.

Background

The International Association of Privacy Professionals (IAPP) defines Data Privacy as "the right to be let alone, or freedom from interference or intrusion and have some control over how personal information is collected and used." Though there is currently no comprehensive federal privacy law in the United States, several states have passed legislation that imposes requirements on how organizations should safeguard personal information and grant specific rights to individuals. As of 2024, all 50 states have passed data breach notification laws, while another 17 have passed data privacy laws.

The following tracker illustrates privacy legislation throughout the country.

State Privacy Legislation Tracker



Source: International Association of Privacy Professionals (IAPP)

A.R.S Article 3 §18-522 – *Anti-identification Procedures* requires government agencies to establish procedures to ensure personally identifying information (PII) cannot be accessed, viewed, or acquired unless authorized by law. Additionally, A.R.S. Article 4 §18-552 – *Breach Notification* requires businesses that incur a data breach to notify affected individuals within 45 days. To comply with A.R.S., the City must know what PII is collected, where it is stored, and how/with whom it is shared. Data privacy should not be confused with data security. Data privacy is focused on the use and governance of personal data, for example, putting policies in place to ensure that consumers' personal information is collected, shared, and used appropriately. Security focuses more on protecting data from malicious attacks and the exploitation of stolen data for profit. While security is necessary for protecting data, it is not sufficient for addressing privacy.

In addition, we assessed the governance of the Privacy Program using the NIST Privacy framework in the following four areas:

- Governance Policies, Processes & Procedures
- Risk Management Strategy
- Awareness & Training
- Monitoring & Review

In 2023, Information Technology Services (ITS) restructured internally so that data security matters are handled by the Information Security Office (ISO) while privacy matters are handled by the Data Privacy Office (DPO). The DPO is led by the Chief Privacy Officer (CPO), who reports to the Chief Information Officer (CIO).

We assessed the compliance of the Privacy Program using existing City Administrative Regulations and IT standards, A.R.S., and the National Institute of Standards & Technology (NIST) Privacy Framework. A full list of privacy related laws and policies is in **Attachment A**.

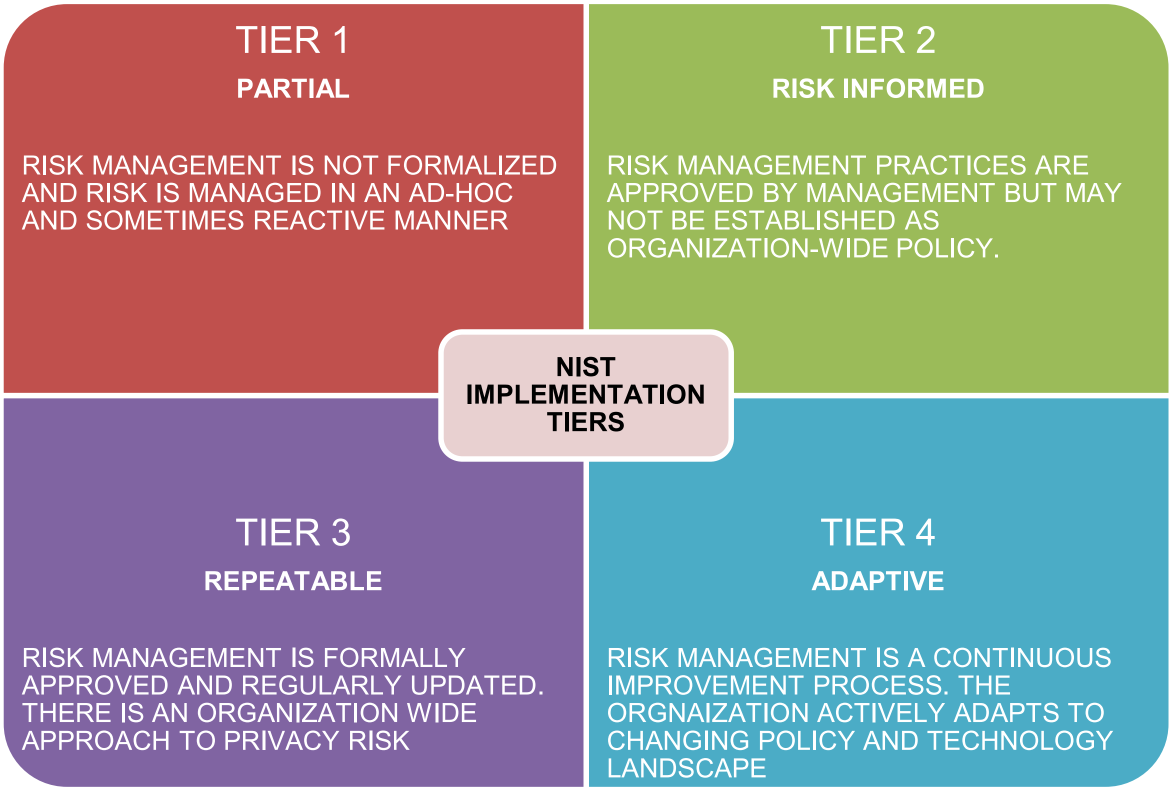
Results in Brief

<u>Overall, the City has made progress identifying weaknesses in the privacy program and is actively working to resolve them.</u>

We measured the maturity of the privacy program using the NIST implementation tiers. An implementation tier allows organizations to gauge their privacy posture and allocate resources to gradually progress to the next tier. Implementation tiers support decision-making and communication about the sufficiency of organizational processes and resources to manage privacy risk.

The chart below describes each of the implementation tiers. The NIST Privacy Framework provides additional guidance.

NIST IMPLEMENTATION TIERS



TIER 1

PARTIAL

RISK MANAGEMENT IS NOT FORMALIZED AND RISK IS MANAGED IN AN AD-HOC AND SOMETIMES REACTIVE MANNER

TIER 2

RISK INFORMED

RISK MANAGEMENT PRACTICES ARE APPROVED BY MANAGEMENT BUT MAY NOT BE ESTABLISHED AS ORGANIZATION-WIDE POLICY.

NIST IMPLEMENTATION TIERS

TIER 3

REPEATABLE

RISK MANAGEMENT IS FORMALLY APPROVED AND REGULARLY UPDATED. THERE IS AN ORGANIZATION WIDE APPROACH TO PRIVACY RISK

TIER 4

ADAPTIVE

RISK MANAGEMENT IS A CONTINUOUS IMPROVEMENT PROCESS. THE ORGNAIZATION ACTIVELY ADAPTS TO CHANGING POLICY AND TECHNOLOGY LANDSCAPE

The City is currently at tier 2 and is working to move into tier 3.

The Chief Privacy Officer (CPO) position has been vacant for over six months. ITS is evaluating staffing and resources to address the responsibilities of the position.

Currently, the CIO serves as the head of the DPO. The CPO is a critical role within the City and is defined in several Administrative Regulations (A.R.). In addition, the CPO is responsible for representing the City in responding to regulatory complaints involving privacy matters. We have been informed that the vacancy created by the CPO's position will likely be used to fill a role in a different leadership position. While there are no immediate plans to backfill the CPO position, ITS is evaluating the steps needed to fill the responsibilities of the position. If the position is not filled, ITS should update the applicable Administrative Regulations to reflect its business practices.

The DPO has procedures in place to monitor privacy legislation. Procedures can be improved by using legal research tools.

The DPO is a two-person function responsible for managing the Citywide governance of the Privacy Program which involves understanding various complex laws and regulations to ensure City compliance. Having a system that can help the DPO perform assessments, perform legal case research, and enforce City standards will help reduce the risk of breach.

A control weakness may allow products/services to be acquired without privacy oversight or evaluation.

The City uses the Business Investment Request Form (BIRF) to gather information regarding technology implementations, including privacy risks, for stakeholder review and approval. The privacy question is optional and is often not completed. While the City reviews information security on all incoming BIRFs, privacy risks may be missed.

ITS has not requested or gathered Information Management Plans (IMP) as required by City policy. ITS has not inquired if departments have updated their plans.

The IMP is the first step in helping departments maintain privacy compliance. *A.R. 1.95 – Information Privacy & Protection* requires each department to update its IMP annually, documenting what personal information they possess and whom it is shared with. The DPO confirmed that they have not enforced IMPs since 2021.

The City does not have formal privacy awareness training for City programs that require privacy compliance.

Privacy is generally embedded into other security-focused training classes or is informal. Some departments may fall under the scrutiny of federal regulations such as the Health Insurance Portability and Accountability Act (HIPAA), the Federal Education Rights and Privacy Act (FERPA), or the Fair Credit Reporting Act (FCRA) and should incorporate industry-level content to train their workforce.

Department Responses to Recommendations

Rec. #: 1.1 Parks & Recreation – Establish procedures to obtain express parental consent before collecting personal information of underage individuals as defined by the Federal Children's Online Privacy Protection Act.	
Response: To comply with this Auditor finding the Parks team submitted RemedyForce ticket 01238108 that would check the box in the system settings that does not allow children under 13 to create an account of pay for the services.	***Target Date:*** Completed
Rec. #: 1.2 ITS – Designate a Chief Privacy Officer (CPO) or update Administrative Regulations to reflect who is responsible for the primary responsibility of the City Privacy Program.	
Response: ITS intends to designate a CPO. It is working with HR on a strategy to create a position and ultimately fill the vacancy.	***Target Date:*** 2/28/2025
Explanation, Target Date > 90 Days: The creation of this position is contingent on HR & CMO approval. Upon approval, creation of this position will require time to work with HR, from drafting of a job description, to posting, and conducting interviews.	
Rec. # 1.3 ITS – Use industry best practices to identify tools that would allow you to perform legal case research and run metrics from privacy impact assessments	
Response: OneTrust, a privacy management platform and Westlaw, a legal research software, were both procured at the end of fiscal year 2024.	***Target Date:*** Completed
Rec. #: 2.1 ITS – Strengthen the Business Investment Request Form process so that privacy issues are reviewed before acquisition.	
Response: ACIOs and DCIOs, including all ITS BIRF reviewers have been trained on what triggers a Privacy BIRF review, as well as what privacy endorsements of a BIRF may look like. That same training is being published to PhxYou for accessibility of all BIRF requesters.	***Target Date:*** 9/1/2024
Rec. #: 2.2 ITS – Update the Information Management Plan template and provide staff training on the new process.	
Response: The IMP template has been updated. A PhxYou training course that corresponds to how to fill out the new IMP template will be created to watch, prior to completing them.	***Target Date:*** 12/31/2025

Explanation, Target Date > 90 Days: Lack of staffing resources will make the creation of an IMP-specific training course challenging. Creation of PhxYOU courses require significant effort on the DPO's part to put together detailed slides, but then also on the HR training course creator, and coordination with PHXTV staff to record the voiceover portion. Coordination with multiple stakeholders in addition to staffing shortages will require additional time for the completion of this recommendation.

Rec. #: 2.3 ITS – Implement a process, supported by documented procedures, to collect updated Information Management Plans from departments at least annually, review the plans, and maintain them in a central repository.

Target Date:

12/31/2026

Response: Conducting the new IMP, which will require explanation and follow up with each of the City's 41 departments and function heads, is a significant effort. We are in the process of hiring a privacy analyst contractor to help us with this. Without the help of a privacy contractor, the DPO would not have resources to complete this due to ongoing competing priorities of program building and enterprise wide privacy consulting. Our ability to complete this recommendation by the target date is contingent on hiring and onboarding that contractor.

Explanation, Target Date > 90 Days: Lack of staffing resources will require the hiring of a contractor privacy analyst. After creation of the job description, and posting it for this niche skill set, we anticipate the role to be filled by 12/31/2025, and then additional time after that to coordinate interviews with 41 City departments and function heads to walk them through expectations of filling out the IMP.

Rec. #: 3.1 – Work with high-risk departments to perform a needs assessment and identify specialized privacy training needs.

Target Date:

7/1/2025

Response: After Gartner creates the risk assessment, we will deploy it City-wide. Afterwards, we will take the results of the assessment, and use it to identify the top five riskiest departments. We will then assess the specialized privacy training needs of those departments.

Explanation, Target Date > 90 Days: Lack of privacy program staffing resources will make the analysis for the need of department-specific training challenging. Due to the demands of program building and privacy consulting for all City departments and limited resources, the DPO will need additional time to assess and identify the training needs of those departments.

Rec. #: 3.2 ITS – Update the current basic privacy awareness training to include content on responsibilities such as notice, choice, consent, collection, use, and disclosure

Target Date:

6/1/2025

Response: New privacy modules are being included in this upcoming year's Security Awareness training to be rolled out October 2024. A Privacy 101 PhxYOU course will be developed and available by the target date.
Explanation, Target Date > 90 Days: Due to the demands of program building and privacy consulting for all City departments and limited resources, the DPO will need additional time to develop the Privacy 101 course. Creation of PhxYOU courses require significant effort on the DPO's part to put together detailed slides, but then also on the HR training course creator, and coordination with PHXTV staff to record the voiceover portion. Coordination with multiple stakeholders in addition to staffing shortages will require additional time for the completion of this recommendation.

1 – Governance Policies Process & Procedures

Background

Governance should be designed to ensure policies, processes, and procedures to manage and monitor the organization's regulatory, legal, environmental, and operational requirements are understood and inform the management of privacy risk.

NIST breaks governance into subcategories described below.

NIST Privacy Framework Governance (GV.PO-P)

Category	Risk Description
Governance Policies Processes & Procedures	Organizational privacy values and policies (e.g., conditions on data processing individuals such as data uses or retention periods, and prerogatives with respect to data processing) are established and communicated.
	Processes to instill organizational privacy values within system/product/service development and operations are established and in place.
	Roles and responsibilities for the workforce are established with respect to privacy.
	Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, and partners).
	Legal, regulatory, and contractual requirements regarding privacy are understood and managed.
	Governance and risk management policies, processes, and procedures address privacy risks.

Summary of the NIST Privacy (Governance) Framework

To determine the effectiveness of governance controls, we performed the following:

- Reviewed a sample of City public websites to check for the presence of a privacy policy.
- Reviewed Administrative Regulations (A.R.) to check for the assignment of roles/responsibilities for managing the Privacy Program.
- Inspected a sample of 3rd party contracts to confirm that they contain terms and conditions for data privacy and data protection.
- Evaluated strategies used by the DPO to keep up to date with privacy legislation.

Results

Privacy policies were displayed but some websites were found to be collecting personal information from children under 13 without parental consent.

A.R. 1.90 – Information Privacy & Protection defines personal information as a name and at least one other piece of information (e.g., e-mail address/date of birth) that could identify an individual. We verified that a privacy policy was posted across a sample of websites that solicit personal information.

Privacy Policy Notice

Department	URL	Privacy Policy Posted
Main Page	www.phoenix.gov/privacy	☑
Library	https://www.phoenixpubliclibrary.org/about/policies	☑
Aviation	https://www.skyharbor.com/aviation-department-privacy-policy/	☑
Parks & Rec	https://www.activenetwork.com/information/processor-privacy-policy	☑
Finance (Payments)	https://www.paymentus.com/privacy-policy/	☑

Policies were posted by the City and/or the service provider in all instances.

The Federal Children's Online Privacy Protection Act (COPPA) requires express parental consent when personal information is collected from individuals under 13. Violators of COPPA may be subject to fines levied by the Federal Trade Commission (FTC). Two of five websites reviewed collect personal information from children under 13 without parental consent:

- **Library** – E-card registration captures name, address, date of birth, and e-mail address. The form did not prompt for consent when a user is under 13.
- **Parks & Recreation** – Active Communities point-of-sale website collects name, e-mail address, and date of birth during registration. The website did not prompt for consent when a user is under 13.

Both websites were missing technical controls during registration that could stop individuals under age 13 from registering on the website. Before the audit closed, we received evidence from the Library Department showing they had added a technical control that requires users under 13 to come into the library with a parent. The Parks & Recreation website has age-restricted programs and is reviewing how controls can be implemented to comply with the COPPA regulations.

The Chief Privacy Officer (CPO) position has been vacant for over six months. ITS is evaluating staffing and resources to address the responsibilities of the position.

Currently, the CIO serves as the head of DPO. The CPO is a critical role within the City and is defined in several A.R's.

Responsibilities of the CPO

City Policy	Responsibilities
A.R. 1.91 – *Information Privacy & Protection*	• Maintain a central repository of IMPs • Investigate potential security breaches
A.R. 1.95 – *Privacy Program*	• Lead the City Privacy Oversight Council • Perform Privacy Risk Assessments • Ensure delivery of privacy training • Oversee compliance with the Red Flag Rules Program
A.R. 1.65 – *Use of GenAI for City Business*	• GenAI Executive Committee Member

The CPO is a critical role in the management of the Privacy Program.

In addition, the CPO is responsible for representing the City in responding to regulatory complaints involving privacy. ITS stated that the vacancy created by the CPO's position will likely be used to fill a role in a different leadership position with no immediate plans to backfill the CPO position. ITS is evaluating the steps needed to fill the responsibilities of the position. If the position is not filled, ITS should update the applicable Administrative Regulations to reflect its business practices.

The City has a process in place to ensure contracts identify the vendor's responsibilities related to data privacy.

All third-party contracts we reviewed included provisions to limit data sharing. *A.R. 1.91 – Information Privacy and Protection* restricts the sharing of personal information for any reason other than one for which it was intended. In addition, departments must include provisions in written contracts requiring data security safeguards; this is achieved through the Data Protection Agreement (DPA) template. The DPA template not only provides language limiting the use of data but mandates requirements for vendors to comply with the State of Arizona breach notification laws. Deviating outside the DPA language may allow external data processors to use data for internal research purposes or sell data without consent. We reviewed a sample of third-party contracts websites across several departments and checked for the presence of data protection language.

Privacy Language in 3rd Party Service Contracts

Department	Contract Number	Description	Purpose use Limitation	Data Protection Language
Fire	CON159338	Captures PHI on cardiac heart monitors.	☑	☑
Human Resources	CON152990	3rd party salary verification service.	☑	☑
Human Services	CON145507	Unemployment data for Gov't programs (TANF, SNAP, etc.).	☑	☑
Library	CON151733	Student data from Phoenix Union High School District	☑	☑
Retirement	CON160020	Pension information for COPERS members.	☑	☑

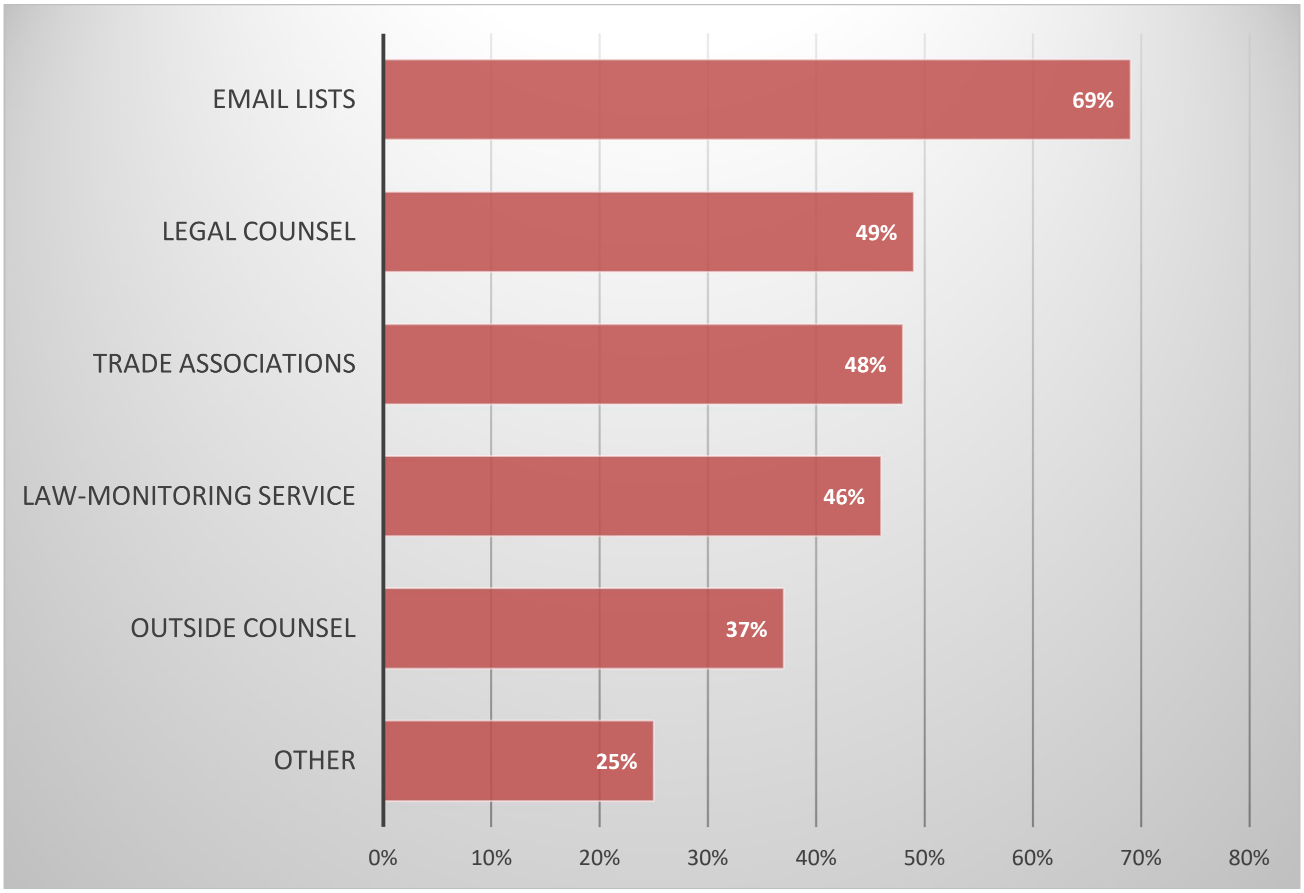
All contracts sampled contained adequate privacy language.

<u>The DPO has procedures for monitoring privacy legislation. Legal research tools can improve these procedures.</u>

According to NIST, organizations should ensure that processes and procedures for assessing compliance with legal requirements are established and in place. The DPO monitors updates in privacy legislation through association memberships, e-mail list subscriptions, and manual research. However, legal research includes the ability to get court decisions that could serve as precedents for future cases. Without legal research, critical tasks such as conducting Privacy Impact Assessments (PIA), may be delayed until the regulatory changes go live. Due to limited staffing, the DPO may benefit from an industry tool that simplifies legal research and allows the department to run data and establish metrics.

In 2023, the IAPP released its annual Privacy Governance report. In the report, 46% of organizations reported having a law-monitoring service that helped perform legal research. We have listed additional methods in the chart below.

Methods used to monitor privacy legislation.



46% of organizations have a law-monitoring service.

Recommendations

1.1 Parks & Recreation – Establish procedures to obtain express parental consent before collecting personal information of underage individuals as defined by the Federal Children's Online Privacy Protection Act.

1.2 ITS – Designate a Chief Privacy Officer (CPO) or update Administrative Regulations to reflect who is responsible for the primary responsibility of the City Privacy Program.

1.3 ITS – Use industry best practices to identify tools that would allow you to perform legal case research and run metrics from privacy impact assessments.

2 – Risk Management Strategy

Background

The NIST Privacy Framework requires that processes to instill organizational privacy values within system/product/service development and operations are established and in place. This is also known as Privacy by Design.

Privacy by Design has the following benefits:

- Build customers' trust by supporting ethical decision-making in product and service design or deployment that optimizes beneficial uses of data while minimizing adverse consequences for individuals' privacy and society as a whole.
- Fulfill current compliance obligations as well as future-proofing products and services to meet these obligations in a changing technological and policy environment.
- Facilitate communication about privacy practices with individuals, business partners, assessors, and regulators.

To support Privacy by Design, the City uses the Business Investment Request Form (BIRF) when departments request to implement new applications. When a department submits a BIRF, and the requestor checks a box disclosing the collection of personal information on the form, the DPO will review it to determine if the application has a privacy risk.

We interviewed personnel and inspected a sample of approved BIRFs across most City departments to validate whether the DPO reviewed the request prior to approval.

Results

Some BIRFs with privacy components were approved without DPO review.

We inspected 10 BIRFs between 2021 and 2024 across a variety of departments with a potential privacy component to determine if DPO reviewed the BIRF. We found 6 of the 10 (60%) requests were not reviewed by the DPO. In our review of the form, we noted that answering the privacy question is optional, and a Privacy Impact Assessment (PIA) is not always performed. Not answering the question may allow new technologies to be implemented without operational safeguards.

The DPO acts in an advisory capacity and departments are ultimately responsible for acting as their own data stewards. Due to limited staffing, the DPO cannot review every incoming BIRF request to determine if there is a privacy concern and relies on departments accurately disclosing a privacy component. Controls should be modified that would make the field mandatory and departments should be trained to accurately fill out the form.

<u>ITS has not collected and reviewed Information Management Plans (IMP) for several years, as required by A.R. 1.90.</u>

A.R. 1.90 – Information Privacy and Protection requires each City department to develop an Information Management Plan (IMP) establishing policies for collecting, managing, and securing personally identifying information (PII) and restricted City information (RCI). Though the policy requires IMPs to be updated annually, it is intended to be a living document, meaning – it should be updated throughout the year as operational needs change. The IMP is the first step in understanding the inventory of data and potential risks. A.R. 1.90 requires the City Privacy Officer to collect plans and hold them in a central repository. During interviews with various departments and staff from ITS, we found that ITS has not collected IMPs for at least three years, and some departments may not be updating their plans annually. The DPO reported that IMPs have not been required since 2021, and they are working on an updated template.

We reviewed a draft version of the new IMP template and confirmed it does include relevant categories such as data collection, data storage, and rights of data subjects.

Recommendations

2.1 ITS – Strengthen the Business Investment Request Form process so that privacy issues are reviewed before acquisition.

2.2 ITS – Update the Information Management Plan template and provide staff training on the new process.

2.3 ITS – Implement a process, supported by documented procedures, to collect updated Information Management Plans from departments at least annually, review the plans, and maintain them in a central repository.

3 – Awareness and Training

Background

The NIST Privacy Framework requires that the organization's workforce and third parties engaged in data processing be provided privacy awareness education and be trained to perform their privacy-related duties and responsibilities. In addition, *A.R. 1.95 – Privacy Program* requires the DPO to develop and deploy basic privacy awareness training.

Designing a training program is not a one-size-fits-all approach. NIST's guidance on Building on Information Technology Security Awareness and Training Program (SP800-50) describes the basics of building an awareness training program. The three most common models are fully centralized, partially decentralized, and fully decentralized, as noted below.

Designing an Awareness Training Program

Fully Centralized Program Management

- Central authority has full control of policy development, strategy and implementation
- Central authority performs needs assessment for all organizational units

Partially Decentralized Program Management

- Central authority shares control of policy and strategy development with organizational units
- Organizational units control training budget, plan and implementation

Fully Decentralized Program Management

- Central authority creates policies
- Organizational units perform the needs assessment
- Organizational units control the strategy training plan, implementation

The City Privacy Program is partially decentralized.

We interviewed departments and examined methods used to provide staff privacy training.

Results

The City does not have a stand-alone basic privacy awareness training course.

At the City level, privacy is generally embedded as a small component in other security awareness training programs. In the most recent version of the security awareness training provided by the Information Security Office and mandated to all employees, privacy was discussed in a 9-minute video clip that shared best practices for working with PII.

At the department level, privacy was delivered through various means. Some departments reported getting privacy training throughout the year with no established frequency or curriculum, while other departments provided employees with a list of departmental policies and asked employees to acknowledge that they read and understood them. This informal method of training may provide awareness but misses the ultimate goal of building the knowledge and skills necessary to facilitate job performance.

In addition, some departments need customized training with content relevant to their industry or regulations in scope. For example, a Library function that receives student data from local high schools may need to train users on the Family Educational Rights to Privacy Act (FERPA), while the Housing Department may need to educate its workforce on rights under the Fair Credit Reporting Act (FCRA). Human Resources personnel who interact with protected health information may need specific training related to HIPAA compliance.

The DPO is in the process of updating the current security awareness training to include a module related to basic privacy awareness. Embedding content that includes employee responsibilities that align with City policies will help make the training effective. Additionally, helping departments establish privacy training for specific compliance areas will reduce the risk of violating federal privacy laws.

Recommendations

3.1 ITS – Work with high-risk departments to perform a needs assessment and identify specialized privacy training needs.

3.2 ITS – Update the current basic privacy awareness training to include content on employee responsibilities such as notice, choice, consent, collection, use, and disclosure.

4 – Monitoring and Review

Background

The NIST Privacy Framework requires policies, processes, and procedures for communicating progress on managing privacy risks to be established and in place. In addition, A.R. 1.95 – *Privacy Program*, requires applicable departments to establish and implement a Red Flags Rule (16 CFR Part 681) program specific to their department line of business to identify and detect the relevant warning signs, or "red flags," of identity theft, take steps to prevent and mitigate the risk of identity theft, and respond appropriately to red flags of identity theft. In response to the rule, ITS issued *City IT Standard b1.9 – Red Flags Rules,* defining key elements and providing guidance to City departments to reduce the risk of identity theft.

The Red Flags Rule applies when an entity:

- **Is a creditor** – a creditor under the rule is one that regularly and in the ordinary course of business obtains or uses consumer reports, furnishes information to credit reporting agencies, or advances funds to or on behalf of a person.
- **Has covered accounts** – An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account.

In 2020, we performed a Red Flags Rule audit and identified four departments (Aviation, Neighborhood Services, Public Transit, and Water Services) that fall under the scope of the rule. These departments defer payment for services (e.g., parking and utility accounts) triggering mandatory compliance with the program. Departments falling under the scope of the Red Flags Rule are required to submit their Red Flags Rule program updates annually to the CPO.

In addition to the Red Flags Rule, A.R.S. 18-552 – *Breach Notification* requires businesses that incur a data breach to notify affected individuals within 45 days. In some cases, notification to the State Attorney General and/or credit reporting agencies is also required.

We reviewed the Red Flags Rules program documentation and documented policies and procedures related to breaches of information to determine if procedures were consistent with applicable laws and regulations.

Results

ITS has received Red Flags Rule program updates for all in-scope departments.

City IT Standard b1.9 – Red Flags Rule requires departments subject to the rule to submit their program updates annually to the CPO. According to the standard, the CPO should use the data to summarize the program to the City Manager and make recommendations for improvement. We reviewed the prior audit and requested all in-scope departments (Aviation, Neighborhood Services, Public Transit, and Water Services) provide a copy of their program update for the most recent calendar year (i.e., 2023). We received evidence showing all four departments complied with the rule. Three of the four departments have not yet completed a program update for the current year but have until November 2024 to do so. The DPO is assessing the ownership of the Red Flags Rule program and intends to update City policies once the review is complete.

IT policies and DPO documented procedures align with the State of Arizona Breach Notification. However, some City documentation references incorrect State statutes.

City IT Standard b1.8 – Privacy Breach Response Plan outlines necessary steps for responding to a data breach and determining whether notification is required. Notification is an important step in all breach investigations. Failure to notify affected individuals can carry civil penalties of up to $500,000 and possible restitution. DPO has documented a 22-step Breach Notification Flowchart that guides the DPO in determining whether notification to State officials and/or credit reporting agencies is required. We were able to map all 22 steps to A.R.S 18-552 – *Breach Notification.*

The Arizona legislature changed the Breach Notification law from A.R.S. 44-7501 to A.R.S. 18-552. We were unable to determine when this occurred but did find references to the old statute in various City systems, including:

- Public-facing website www.phoenix.gov/its/privacy
- City IT Standard b1.7 – *Information Privacy Program*
- City IT Standard b1.8 – *Privacy Breach Response Plan*

The DPO should update these items to reflect current Arizona Revised Statutes.

Recommendation

None

Attachment A – Privacy Related City Policies and Arizona Revised Statutes

Policy	Source	Description
A.R. 1.63 – *Electronic Communications & Information Acceptable Use*	City Policy	Communicates no expectation of privacy for City employees using City systems.
A.R. 1.65 – *Use of Generative AI*	City Policy	Governs responsible use of Artificial Intelligence (AI)
A.R. 1.90 – *Information Privacy & Protection*	City Policy	Securing & protecting personally identifying information (PII)
A.R. 1.11– *Information Privacy & Protection Supplement*	City Policy	Provides guidance for sharing personal information with 3rd parties
A.R. 1.95 – *Privacy Program*	City Policy	Establishes authority over the City Privacy Program
B1.7 – *Information Privacy Program*	City IT Policy	Requires privacy Risk Assessment for City departments
B1.9 – *Red Flags Rule*	City IT Policy	Requires controls that detect identity theft
18-522 – *Arizona Anti-identification Procedures*	Arizona Revised Statutes	Requires government agencies to protect PII
18-552 – *Arizona Breach Notification Law*	Arizona Revised Statutes	Requires notification due to breach of personal information

Scope, Methods, and Standards

Scope

We assessed the current state of the Privacy Program against the City's privacy policies, Arizona Revised Statutes, and industry standards such as the NIST Privacy Framework.

The internal control components and underlying principles that are significant to the audit objectives are:

- Control Environment
  - The oversight body and management should demonstrate a commitment to integrity and ethical values.
  - The oversight body should oversee the internal control system.
  - Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.
  - Management should demonstrate a commitment to recruit, develop and retain competent individuals.
- Risk Assessment
  - Management should define objectives clearly to enable the identification of risks and define risk tolerances.
  - Management should identify, analyze, and respond to significant changes that could impact the internal control system.
- Control Activities
  - Management should design control activities to achieve objectives and respond to risks.
  - Management should design the entity's information system and related control activities to achieve objectives and respond to risk.
- Information & Communication.
  - Management should externally communicate the necessary quality information to achieve the entity's objectives.
- Monitoring Activities
  - Management should remediate identified internal control deficiencies on a timely basis.

Methods

We used the following methods to complete this audit:

- Reviewed the CIPP/US Privacy course provided by the International Association of Privacy Professionals (IAPP).
- Reviewed the NIST Privacy Framework.
- Reviewed City policies related to the governance of the Privacy Program.
- Interviewed members of the Data Privacy Office (DPO).
- Interviewed a sample of City Departments.
- Inspected contract documentation and City websites to check for privacy language.

Unless otherwise stated in the report, all sampling in this audit was conducted using a judgmental methodology to maximize efficiency based on the auditor's knowledge of the population being tested. As such, sample results cannot be extrapolated to the entire population and are limited to a discussion of only those items reviewed.

Data Reliability

The scope of this audit was to validate the governance of the Privacy Program against industry standards. We did not require the use of data sets to perform our evaluation.

Standards

We conducted this performance audit in accordance with generally accepted government auditing standards. 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. Any deficiencies in internal controls deemed to be insignificant to the audit objectives but that warranted the attention of those charged with governance were delivered in a separate memo. We are independent per the generally accepted government auditing requirements for internal auditors.