Office of the
Internal Auditor

ENGAGEMENT REPORT

January 2025

Privacy Advisory

CITIZENS
PROPERTY INSURANCE CORPORATION

Table of Contents: Page

Executive Summary

Background

Privacy processes and procedures are fundamental to the organization's ability to perform critical business functions and uphold compliance with ever-evolving legal and regulatory mandates. The growing complexity of privacy risks, driven by emerging cybersecurity threats, rapid technological advancements, and increasingly stringent statutory obligations, necessitates a proactive and adaptive approach to data protection.

A mature privacy function establishes and enforces a robust privacy framework across all applications, tools, and business units, ensuring comprehensive adherence to legal requirements and industry best practices. This framework enhances compliance and improves the organization's agility and operational efficiency by embedding privacy considerations directly into core processes. Such an integrated approach empowers the organization to safeguard proprietary and customer data effectively, build and sustain stakeholder trust, and preserve its reputation. Ultimately, a well-executed privacy program is critical to the organization's long-term success, strategic risk management, and ability to navigate the complex landscape of data privacy and protection effectively.

Objectives and Scope

Internal Audit through this engagement provided support to the Chief Privacy Officer by evaluating the current privacy program and developing a comprehensive privacy framework to support a strong privacy culture among Citizens. This includes comparing Citizens' current processes, structure, and capabilities within privacy to leading practices. These areas are included in the scope:

- Applied Frameworks and Maturity
- Current Controls and Activities
- Mission-critical data types and areas
- Application of and conformance to required regulations

Engagement Results

Internal Audit's assessment of the current Privacy Program identified several opportunities for enhancement:

Current State	Proposed Enhancements
There is no explicit privacy framework outlining the processes, responsibilities, and activities associated with Privacy.	Create a comprehensive Privacy Framework Program.
No method to perform National Institute of Standards and Technology (NIST) Privacy, or relevant standard conformance/implementation validation and or a maturity assessment within the organization.	Leverage the current Laws, Rules and Regulations (LRR) Compliance model and build procedures for the Privacy function.

Executive Summary

There is no explicit method to monitor the improvement of privacy practices.	Leverage the current LRR model, risk rank areas of lower maturity, and work with business units to improve and/or mitigate.

Implementation of the following proposed enhancements will significantly improve the privacy function's impact, efficiency, and effectiveness.

1. **Create a comprehensive Privacy Program Framework** – Citizens has an established Information Security and Privacy Policy (#400) which at a high level contains the elements listed below. However, an explicit and independent Privacy Program Framework and baseline procedures will benefit Privacy by outlining the process and promoting active privacy controls within the organization. This program should:
   - Define overarching goals and contain a statement of purpose.
   - Identify, define, and contextualize the elements of an effective privacy program.
   - Explain the structure and oversight of the privacy function
   - Describe processes/activities that will be employed to perform internal monitoring and review of privacy practices (including a privacy certification process).
   - Discuss methods of violation reporting available to the business.

   As part of this engagement, Internal Audit worked in conjunction with the Privacy Office to develop a draft framework that outlines all the above requirements. This draft framework has been delivered to the Chief Privacy Officer for review and implementation.

2. **Establish a method for maturity assessment, conformance validation, and active improvement of privacy practices against the NIST Privacy Framework or relevant standard** – Utilizing the current LRR process as a baseline, develop a method to perform the above activities required of a privacy function. This includes:
   - Systematic and consistent maturity assessments against the NIST Privacy framework or relevant standard throughout the organization. This should take place at least annually. During this engagement, the Chief Privacy Officer performed the first of these assessments and was given feedback by OIA.
   - Utilizing the annual assessment, identifying areas of high-risk requiring improvement/mitigation and working with the business functions to understand and improve. Giving the privacy function clear activity areas of focus each period.
   - Tracking maturity over time to produce measurable results that map the maturity lifecycle of the privacy program.
   - Working with the Executive Leadership Team to determine priorities and focus.
   - Establishing authority and autonomy for the privacy function as a whole.

   As part of this engagement, Internal Audit worked in conjunction with Risk and Controls, Compliance, and the Privacy Officer to walk through the current LRR process performed by Compliance in Audit Board. Building a similar workstream for privacy will allow the Privacy Office to perform the above-mentioned functions. Internal Audit also recommends that Privacy, in conjunction with relevant stakeholders, determine the most effective privacy standard to

Executive Summary

follow. Further, management should consider NIST Privacy adoption as a baseline framework and clearly document any deviations as business needs arise.

In conclusion, Internal Audit will continue to support the Privacy Office in this effort. Once the above recommendations are implemented and established, OIA encourages management to consider the resources available to the Privacy Office to determine the ability to perform their functions.

We thank management and staff for their cooperation and professional courtesy throughout this engagement.

Executive Summary

Addressee(s) Chuck Bowen, Chief Privacy Officer

Business Leaders:
Tim Cerio, Chief Executive Officer
Brian Newman, Chief Legal Officer & General Counsel
Mark Kagy, Inspector General

Audit Committee:
Jamie Shelton, Citizens Audit Committee Chair
Carlos Beruff, Citizens Audit Committee Member and Chairman of the Board
Scott Thomas, Citizens Audit Committee Member

Following Audit Committee Distribution:
The Honorable Ron DeSantis, Governor
The Honorable Jimmy Patronis, Chief Financial Officer
The Honorable John Guard, Chief Deputy Attorney General
The Honorable Wilton Simpson, Commissioner of Agriculture
The Honorable Ben Albritton, President of the Senate
The Honorable Daniel Perez, Speaker of the House of Representatives

The External Auditor

Completed by Kyle Sullivan, Assistant Director

Under the Direction of Joe Martins, Chief of Internal Audit