PUBLISHED

Office of the
Internal Auditor

Engagement Report

May 2026

Identity Governance and Access Management

This report is a redacted version of a Restricted Confidential audit report. Certain information has been removed or summarized to comply with confidentiality and exemption requirements under Florida Statutes s.627.352.

CITIZENS
PROPERTY INSURANCE CORPORATION

Table of Contents:

This report is a redacted version of a Restricted Confidential audit report. Certain information has been removed or summarized to comply with confidentiality and exemption requirements under Florida Statutes s.627.352.

Executive Summary

Background

Identity Governance and Access Management (IGA/IAM) is a critical component of Citizens' cybersecurity, operational risk, and control framework. Effective IGA/IAM helps ensure that access to systems, applications, and data is appropriately authorized, periodically reviewed, and aligned with users' job responsibilities and business needs. Strong identity governance also helps prevent unauthorized, inappropriate, or excessive access that could increase the risk of data exposure, fraud, operational disruption, regulatory noncompliance, or ineffective segregation of duties.

As Citizens continues to rely on enterprise applications, third-party platforms, cloud-based services, and automated access processes, consistent governance over user identities and access privileges is essential. Clearly defined roles, documented policies and procedures, effective oversight, and timely monitoring help support accountability across Information Technology, Information Security, business units, application owners, and third-party service providers. These controls also support compliance with applicable laws, regulations, internal policies, and industry standards.

Objectives and Scope

The engagement evaluated whether a formal IGA/IAM governance model is established, clearly defined, and consistently enforced to support appropriate oversight of user access to Citizens' systems and data.

The scope of the engagement included an assessment of:

- The overall IGA/IAM governance framework, including committees, oversight bodies, and reporting structures.
- Roles and responsibilities for identity and access management across Information Technology, Information Security, business units, application owners, and third-party providers.
- Segregation of duties within the governance and administration of access management processes.
- Accountability for key IGA/IAM functions, including access provisioning, access reviews, policy enforcement, and exception management.
- The existence, communication, and enforcement of formal policies and supporting procedures for identity lifecycle management.
- Training and awareness related to IGA/IAM responsibilities for relevant stakeholders.

Results

Overall, management has established a documented IGA/IAM governance framework that defines responsibilities for access monitoring, access design, segregation of duties requirements, and policy enforcement. Policies and procedures also outline roles and expectations related to application access management. In addition, management has established several oversight bodies that support technology and access governance, including the IT Governance Committee, the System Development Life Cycle group, the Architecture Review Committee, and other relevant groups.

This report is a redacted version of a Restricted Confidential audit report. Certain information has been removed or summarized to comply with confidentiality and exemption requirements under Florida Statutes s.627.352.

Executive Summary

While the governance structure and foundational documentation are in place, Internal Audit identified three medium-risk opportunities to improve the consistency and effectiveness of management's execution of established IGA/IAM policies and procedures.

Conclusion

Internal Audit concluded that Citizens has established foundational IGA/IAM governance elements, including documented policies, defined oversight bodies, and assigned responsibilities. However, opportunities exist to strengthen consistent execution, communication, monitoring, and enforcement of established IGA/IAM requirements.

The observations identified during this engagement have been discussed with management, and management has agreed to corrective actions. Internal Audit will monitor remediation activity through the established audit issue follow-up process.

We would like to thank management and staff for their cooperation and professional courtesy throughout this audit.

Distribution

Addressee(s) Tim Craig, CISO – Information Security

Business Leaders:
Tim Cerio, President/CEO/Executive Director
Aditya Gavvala, Chief Information Officer
Brian Newman, Chief Legal Officer
Mark Kagy, Inspector General

Audit Committee:
Jamie Shelton, Audit Committee Chair
Carlos Beruff, Audit Committee Member and Chairman of the Board
Robert Spottswood, Audit Committee Member

Following Audit Committee Distribution:
The Honorable Ron DeSantis, Governor
The Honorable Blaise Ingoglia, Chief Financial Officer
The Honorable James Uthmeier, 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, Internal Audit Director, under the Direction of Joe Martins, Chief of Internal Audit.

This report is a redacted version of a Restricted Confidential audit report. Certain information has been removed or summarized to comply with confidentiality and exemption requirements under Florida Statutes s.627.352.