PUBLISHED

Office of the
Internal Auditor

Engagement Report

October 2025

Backup & Recovery of Critical Systems

CITIZENS
PROPERTY INSURANCE CORPORATION

Table of Contents: Page

Executive Summary

Background

Backup and recovery capabilities for critical systems are a key component of Citizens' resiliency approach to ensure timely and adequate recovery from adverse events. This enables Citizens to resume business operations to serve policyholders and other stakeholders. Citizens increasingly rely on Software as a Service (SaaS) for many solutions. This shifts responsibility for backup and recovery capabilities from Citizens to vendors and their sub-vendors. Backup and recovery also play a key role in hardening Citizens' environments from possible ransomware attacks through the recoverability of data that is encrypted by hostile parties.

Objectives and Scope

The objective of this engagement was to assess the design and operating effectiveness of backup and recovery controls supporting critical systems and to evaluate whether backup and recovery capabilities adequately support business continuity and cyber resilience objectives. This review further verified the adequacy of resiliency features provided by cloud vendors and sub-vendors that Citizens depends on for resiliency purposes.

The engagement evaluated backup and recovery capabilities for critical on-premises systems and SaaS. The review included the following areas:

- Activities managed primarily by IT:
    - Virtual backup configurations and policies for Citizens managed on-premises systems
    - Frequency, completeness, and success of restore testing of virtual backups of on-premises systems
    - Design and adequacy of ransomware recovery capabilities for the network file storage solution
    - Integration of backup, restore and ransomware solutions with enterprise monitoring, alerting, and incident response processes
- Activities managed primarily by Resiliency:
    - Classification and risk ranking of systems supporting business operations, including the criteria used
    - Alignment of backup and recovery strategies and capabilities with overall business resiliency and continuity planning
    - Oversight and performance review of the backup and recovery capabilities of SaaS vendors and sub vendors, including service commitments, SLAs, and independent assurance reports (system and organizational controls)

This engagement was not a comprehensive disaster recovery and business continuity review. Instead, it focused on specific activities performed by the Storage and Resilience teams, as outlined in the aforementioned.

Results

Internal Audit confirmed that the Storage Team proactively monitors storage, backup and restore tools daily. The IT teams also consistently report relevant incidents to the service management platform. Management is proactively working on identifying next-generation backup and restore tools. The Resilience Team has successfully implemented the business continuity module of the

Executive Summary

service management platform and continues to strengthen Citizens' resiliency capabilities. The Resilience Team has made significant progress in establishing and updating technical and business impact assessments and linking these to disaster recovery and business continuity plans.

Management self-reported known minor improvement opportunities during this engagement.

Conclusion

Following the completion of Internal Audit's planning and insight into the population of critical systems, Internal Audit selected a sample for review. Internal Audit also verified the existence and effectiveness of controls recommended by leading practices and prescribed by Citizens' governing documents. Internal audit identified 1 medium risk finding which was discussed and agreed upon with management. Internal Audit also recommended multiple improvement opportunities to strengthen internal controls to management.

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

Distribution

Addressee(s)

Sudheer Kondabrolu, Director – IT Infrastructure
Daniel Rich, Mgr – Systems Engineering
Becky Davis, Mgr – Asst Director – Business Systems Resiliency & Data Gov.

Business Leaders:
Tim Cerio, President/CEO/Executive Director
Aditya Gavvala, Chief Information Officer
Jennifer Montero, Chief Financial Officer
Spencer Kraemer, Sr Director – Vendor Management & Purchasing
Keri Dennis, Asst Director – Vendor Relationship Mgmt
Brian Newman, Chief Legal Officer & General Counsel
Tim Craig, VP – Chief Information Security Officer
Michael Maitland, Asst Director – Enterprise Records Management
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 Peter Schellen, Internal Audit Manager and Kyle Sullivan, Director – Internal Audit. Under the Direction of Joe Martins, Chief of Internal Audit.