OIA
OFFICE OF THE INTERNAL AUDITOR

CITIZENS
PROPERTY INSURANCE CORPORATION

INTERNAL AUDIT

System and Information Backup Audit Report

November 19, 2019

Report Number: 2019-IT-AUD-06 System and Information Backup

Table of Contents

Executive Summary

Background

Citizens' ability to successfully backup and restore data in the event of a disruption is critical to our ability to sustain ongoing operations and service policyholders.

Backups are crucial in situations such as:

- A database table is accidently or otherwise deleted from a production database and it needs to be restored to resume normal business activities.
- A user accidentally deletes a file from a shared drive.
- One or more servers fail due to a software update problem and must be restored to the operational state in effect prior to the start of the update.
- One or more servers, systems or data is impacted by ransomware or other malware.
- A disaster renders the primary data center unusable and production must be resumed in an alternative data center.

System and information backups are an important component of Citizens' Business Continuity, Disaster Recovery (DR) and IT Resiliency plans and capabilities. System backups involve making point-in-time copies of all data on a given system. Suitable backup solutions can restore anything from a single file to an entire system, to a recent, 'known good' state. Backups are stored on a large data storage system which uses hi-speed rotating disks, and magnetic tape is primarily used for off-site, long-term storage. Consideration is being given to cloud backup in the future, where a copy of a physical or virtual file or database is sent to a secondary, off-site location for preservation in case of equipment failure or catastrophe.

Citizens' Information Technology Infrastructure team maintains the backup systems, performs backup procedures for systems and data, and conducts periodic testing to ensure the backups can be successfully restored.

Audit Objectives and Scope

The objective of this audit was to evaluate the effectiveness of processes associated with system and data backups. The scope of the audit included an assessment of controls in the following areas:

- Backup procedures and processes
- Access controls for backup systems and saved backups
- Monitoring of backup jobs and resolution of failed jobs
- Validation that business-critical systems and information are included in backups
- Retention of backups, both onsite and at the offsite tape library
- Testing of backups

Excluded from the scope of this audit are processes related to the replication of systems and data from the production co-location data center to the disaster recovery co-location data center, which serves as the primary method of recovery in a disaster event. These processes are tested

Executive Summary

periodically by IT and business representatives as part of the Business and Systems Resiliency disaster recovery exercises and are separate from the backup systems and processes.

Management's Assessment and Reporting on Controls

Internal Audit (IA) provided IT management an opportunity to share known control weaknesses and their plans to remediate them. This process is intended to foster an environment whereby management and staff conduct periodic proactive reviews of controls and are aware of the risks to the business. It also enables us to focus our audit efforts on areas where it can add value to the organization. At the start of the audit, IT management self-identified areas where additional controls should be designed. These include:

- **The backup request process is not automated.**

  A backup request must be submitted by a server owner. Reliance upon the server owner can lead to servers not being backed up if errors occur. With the implementation of the new service management system, the workflow will be automated by year-end 2019 to create backup requests for all new servers.

  This change does not affect current servers and IA suggests that consideration should be given to automate the backup process in all instances.

- **Full system backups are not performed for physical servers which comprise approximately 6% of the production environment and some virtual servers**.

  Without full system backups, failed servers would have to be rebuilt, beginning with the installation of the operating system, applying configuration settings, and installing the applications. In-house talent to rebuild the systems quickly may not be available. Legacy applications operating on legacy servers may encounter an extended outage if a significant event would occur. These legacy systems are not targeted for long term use. IT Management is developing a new backup strategy that will consider these opportunities.

- **One of the production backup systems is running an unsupported version of the backup software.**

  IT management believes that vendor support may be available at a cost, if needed. A project is underway to upgrade the system by year-end 2019.

Audit Opinion

IA confirmed that staff responsible for backup and recovery is knowledgeable about systems and processes. Adequate controls have been implemented for the monitoring of backup jobs and restoration testing of the backups from the data storage system. Although there is currently a staff shortage, staff continues to manage the area well.

Our work indicated certain areas where management should consider strengthening the current control environment to ensure that Citizens, under any circumstances, is in a position to reconstruct and repair broken services with a well-managed back-up and recovery process in place:

Executive Summary

- **Some critical servers were either not backed up regularly or backed up at all.**

  Although management confirmed that the backup request process is manual and recognizes that potential control weaknesses, IA noted that some servers were not backed up regularly or at all. A process to reconcile or validate required backups has not been implemented.

- **Physical backup tapes are not periodically tested to ensure usability.**

  Because backup tapes are a significant part of operational recovery requirements and business continuity, a formal test process should be implemented that ensures the availability of tapes if needed.

- **System account passwords for the storage device are shared by the backup and recovery staff.**

  The system administrator account and a system service account for the backup storage device are being shared by the staff. The IT Security Standard requires a method to ensure accountability to individual users when using system related accounts. IT instituted system changes during the audit to align practice to policy.

Management agrees with the observations and has developed action plans to implement appropriate processes and controls in these areas. Additional minor process improvement opportunities were also discussed with management for consideration.

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

Appendix 1

Issue Classifications

Control Category	High	Medium	Low
Financial Controls (Reliability of financial reporting)	• Actual or potential financial statement misstatements > $10 million • Control issue that could have a pervasive impact on control effectiveness in business or financial processes at the business unit level • A control issue relating to any fraud committed by any member of senior management or any manager who plays a significant role in the financial reporting process	• Actual or potential financial statement misstatements > $5 million • Control issue that could have an important impact on control effectiveness in business or financial processes at the business unit level	• Actual or potential financial statement misstatements < $5 million • Control issue that does not impact on control effectiveness in business or financial processes at the business unit level
Operational Controls (Effectiveness and efficiency of operations)	• Actual or potential losses > $5 million • Achievement of principal business objectives in jeopardy • Customer service failure (e.g., excessive processing backlogs, unit pricing errors, call center non responsiveness for more than a day) impacting 10,000 policyholders or more or negatively impacting a number of key corporate accounts • Actual or potential prolonged IT service failure impacts one or more applications	• Actual or potential losses > $2.5 million • Achievement of principal business objectives may be affected • Customer service failure (e.g., processing backlogs, unit pricing errors, call center non responsiveness) impacting 1,000 policyholders to 10,000 or negatively impacting a key corporate account • Actual or potential IT service failure impacts more than one application for a short period of time	• Actual or potential losses < $2.5 million • Achievement of principal business objectives not in doubt • Customer service failure (e.g., processing backlogs, unit pricing errors, call center non responsiveness) impacting less than 1,000 policyholders • Actual or potential IT service failure impacts one application for a short period of time

Appendix 1

Control Category	High	Medium	Low
	and/or one or more business units • Actual or potential negative publicity related to an operational control issue • An operational control issue relating to any fraud committed by any member of senior management or any manager who plays a significant role in operations • Any operational issue leading to death of an employee or customer	• Any operational issue leading to injury of an employee or customer	
Compliance Controls (Compliance with applicable laws and regulations)	• Actual or potential for public censure, fines or enforcement action (including requirement to take corrective actions) by any regulatory body which could have a significant financial and/or reputational impact on the Group • Any risk of loss of license or regulatory approval to do business • Areas of non-compliance identified which could ultimately lead to the above outcomes • A control issue relating to any fraud committed by any member of senior management which could have an	• Actual or potential for public censure, fines or enforcement action (including requirement to take corrective action) by any regulatory body • Areas of non-compliance identified which could ultimately lead to the above outcomes	• Actual or potential for non-public action (including routine fines) by any regulatory body • Areas of noncompliance identified which could ultimately lead to the above outcomes

Appendix 1

Control Category	High	Medium	Low
	important compliance or regulatory impact		
Remediation timeline	• Such an issue would be expected to receive immediate attention from senior management, but must not exceed 60 days to remedy	• Such an issue would be expected to receive corrective action from senior management within 1 month, but must be completed within 90 days of final Audit Report date	• Such an issue does not warrant immediate attention but there should be an agreed program for resolution. This would be expected to complete within 3 months, but in every case must not exceed 120 days

Appendix 2

Distribution

Addressee(s) Thomas Dubocq, Director, IT Infrastructure

Addressee(s) **Business Leaders:**
Barry Gilway, President/CEO/Executive Director
Kelly Booten, Chief, Systems and Operations
Aditya Gavvala, V.P., IT Services and Delivery
Christine Turner Ashburn, Chief, Communications, Legislative & External Affairs
Mark Kagy, Acting Inspector General

Audit Committee:
Marc Dunbar, Citizens Audit Committee Chair
Bette Brown, Citizens Audit Committee Member
James Holton, Citizens Audit Committee Member

Following Audit Committee Distribution:
The Honorable Ron DeSantis, Governor
The Honorable Jimmy Patronis, Chief Financial Officer
The Honorable Ashley Moody, Attorney General
The Honorable Nikki Fried, Commissioner of Agriculture
The Honorable Bill Galvano, President of the Senate
The Honorable Jose R. Oliva, Speaker of the House of Representatives

The External Auditor

Audit performed by Karen Wittlinger, IT Audit Director and Gary Sharrock, IT Audit Manager

Under the Direction of Joe Martins, Chief of Internal Audit