Office of the Internal Auditor

Advisory Memorandum

March 2022

Check Printing Software Implementation

Memorandum Number: 2022-MAS-02
Check Printing Software Implementation

CITIZENS
PROPERTY INSURANCE CORPORATION

Advisory Memorandum

Background

During 2021 Citizens procured and implemented CheckPlus, a check printing software that allows the ability to print return premium, commission, and claims checks. The check printing software eliminates the need to buy, store, and protect preprinted checks and allows for a secure payment process. Additionally, this software integrates with host applications Guidewire BillingCenter and ClaimCenter.

Check processing starts within the host applications, which produce check files that are used by the check printing software, processed through unique check templates, and sent to check printers located in the Jacksonville and Tallahassee offices. Citizens prints approximately 40,000 checks per month through this process. Appropriate system access and user control considerations prevent unauthorized access and create opportunities to properly segregate incompatible job responsibilities.

In addition, the service contract on the two-high speed MICR check printers currently used will expire in June 2022. As a result, a project to procure replacement high speed MICR printersis in progress, which will be compatible with the CheckPlus software.

Objectives and Scope

The objective of this advisory engagement was to evaluate the initial user access configuration to confirm that the processes and controls are in place to monitor and manage user access and the related provisioning of the new check printing software, CheckPlus. Additionally, Internal Audit considered segregation of duties.

Our scope included a review of the following areas:

- System Access
- Segregation of Duties

The new check printing software is used to process return premium, commission, and claims checks paid through BillingCenter and ClaimCenter. Whereas payments made through Centerpoint use the check printing capabilities built within CenterPoint.

Results

Results from our review indicate that CheckPlus has adequate access control capabilities and mechanisms, which allow for granting/restricting access to individual users and/or groups by assigning them rights. Additionally, Internal Audit validated that system users are appropriately segregated within the process.

Our review indicated, during the implementation of the system, some users were provided privileged access to facilitate a smooth transition and efficiently troubleshoot items as they occurred. Specifically, we observed two user id's with generic user account names ("Supervisor" & "Admin") both with significant access and rights to the system. The Supervisor user ID is a shared user ID used by 8 individuals; while the Admin user ID is used by the vendor to access the system. Additionally, we noted three users, all CPIC employees, who were assigned privileged access and rights to the system. Logging and monitoring capabilities are available; however, monitoring processes have not been implemented. Although the access was originally intended to be granted

temporarily during implementation this was not changed or removed after implementation and is currently in conflict of the Information System Access Management Policy.

The Information System Access Management policy (#400-AM) requires that:

- All users shall have a unique User ID for their personal use only.
- All users must not attempt to share their User IDs and passwords.
- Use of generic or shared user accounts is expressly prohibited unless a risk acceptance/exception is approved following existing exception to policy processes.
- The use of information system accounts must be monitored as appropriate to the risks associated with use. Information Owners (as defined by the Information Security and Privacy Policy) must identify activities of significant impact/risk that should be logged by the application and archived for audit/review purposes.
- Special attention shall be given to the allocation of privileged access rights, which allow users to override system controls. Access administration records must be maintained, and those records will provide an audit trail of authorization; account creation; adjustment allowing for role changes; changes to access privileges; and account closure.

The failure to restrict access appropriately, along with not properly monitoring administrator activity, may cause data loss and/or data corruption if unauthorized edits and/or deletions within the system were to occur.

In discussion with the Director of IT Security & Risk, the specific guidance referenced above provides principles to Management for adequate system access management and monitoring. We suggest that Management work closely with IT Security Risk and Compliance to ensure these risks are adequately monitored and remediated. Management has begun proactive remediation efforts.

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

Distribution

Addressee(s) Angela Lockwood, Director – Product Management

Business Leaders:
Barry Gilway, President/CEO/Executive Director
Christine Turner Ashburn, Chief, Communications, Legislative & External Affairs
Jennifer Montero, Chief Financial Officer
Jay Adams, Chief - Claims
Mark Kagy, Inspector General

Audit Committee:
Erin Knight, 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 Ashley Moody, Attorney General
The Honorable Nikki Fried, Commissioner of Agriculture
The Honorable Wilton Simpson, President of the Senate
The Honorable Chris Sprowls, Speaker of the House of Representatives

The External Auditor

Completed by Patrick Lynch, Internal Audit Manager
Under the Direction of Joe Martins, Chief of Internal Audit