OIA
OFFICE OF THE INTERNAL AUDITOR

CITIZENS
PROPERTY INSURANCE CORPORATION

INTERNAL AUDIT

Centerpoint HCM User Access Audit Report

September 07, 2018

Report Number: 2018-AUD-38 Centerpoint HCM User Access

Table of Contents

Executive Summary

Background

In 2016, Oracle Fusion Cloud Service, an integrated ERP solution, was purchased to support Citizens' strategic goal to ensure a strong financial operating environment. The Oracle integrated ERP solution, branded by Citizens as Centerpoint, replaces independent applications previously used by individual departments. The Centerpoint project consists of five phases with implementation dates ranging from April 2017 through November 2018. Two of the five phases focused on Human Resources:

- Phase 4, Human Capital Management (HCM) functions, such as benefits, payroll, time and absence management, and talent acquisition went live in December 2017.
- Phase 5, Advanced HCM functions for talent management and performance management went live in June 2018.

The HCM module within the Centerpoint application is utilized to enter, process, and manage payroll, benefits, time and labor, and talent management for Citizens. Privileged roles within the HCM module allow an assigned user the ability to create and modify employees' salaries, benefits, addresses, and bank accounts. Access management includes creating, modifying, terminating, and monitoring user access, roles, and permissions. Designated business owners, access managers, and an access provisioning team are collectively responsible for access management control. Continued maintenance and recertification are necessary to ensure user access to information remains appropriate.

Audit Objectives and Scope

The objective of this audit was to evaluate the adequacy and effectiveness of access controls for the Centerpoint HCM module. The scope of the audit included an assessment of controls for the following areas:

- User provisioning of new hires and role changes due to promotions, demotions, lateral moves or changes in job duties
- User de-provisioning of voluntary and involuntary terminations
- Segregation of duties
- Monitoring activities
- Security of confidential data

Audit Opinion

The overall effectiveness of the controls evaluated during the audit of Centerpoint HCM User Access is rated as **Needs Improvement.**

Results from our audit work indicate that Human Resources, Information Technology, and the Centerpoint Project Team proactively collaborated to design and implement appropriate user access

Executive Summary

controls and to properly secure confidential data. However, system limitations, the complexity of Oracle roles and permissions, and the business need to create custom roles contributed to challenges in effectively managing user access.

OIA noted the following control deficiencies that need to be addressed:

- **HCM roles and permissions are not clearly defined resulting in instances of inadequate segregation of duties and excessive permissions that are not adequately monitored.** Individuals were assigned to conflicting roles within the HCM module that do not properly segregate duties and/or exceed the minimum necessary to perform the user's job responsibilities as a result of the complexity of the Oracle hierarchy. The roles and permissions include the ability to create an employee and update payroll data including changes in pay rates and bank account information. In addition, activities performed by these users are not specifically logged or monitored which may result in inappropriate transactions not being detected in a timely manner. Granting access to unnecessary privileges and creating unnecessary roles can compromise the security of data and may lead to disclosure of confidential or sensitive information, loss of data integrity, loss of proprietary information, business or system disruption, and fraudulent activity.
- **The design and use of the HCM firecall Account to perform emergency administrative tasks does not align with the standard Citizens' firecall process.** The HCM Application Administrator role is assigned to users on a temporary as-needed basis, for firecall access by a special User Access Management (UAM) ticket through the Service Desk application. The role is to be removed once the purpose for which it was assigned has been fulfilled, usually 24 hours. Assignment of the role is not restricted to the limited timeframes necessary to only perform the emergency tasks. Inappropriate access to the production environment could result in unauthorized modifications potentially leading to financial loss.
- **Access to employee restricted and sensitive information is not adequately protected.** Five shared network folders containing restricted and sensitive employee information are not encrypted or password protected and IT personnel have access based on their administrative roles. The current process does not adhere to the Citizens Information Classification and Handling Policy. Failure to adequately restrict access to employee information could result in misuse of information.
- **User access changes and terminations were not processed timely.** A small number of users that should be deactivated remain active in the Citizens Authentication Gateway (CAG). Access for the users was granted outside of the Service Desk process which caused the user profile to be inappropriately updated and impacted the user deactivation process. Delays were also noted in the timeliness of the submission and processing of User Access Management (UAM) tickets to remove privileged roles from two users. Failure to terminate

Executive Summary

user access in a timely manner may lead to disclosure of confidential or sensitive information, business or system disruption, and unauthorized transactions.

As management implements their corrective action plans to mitigate the risks identified, additional monitoring controls should be considered to ensure independent oversight is performed for individuals who will continue to have access to sensitive and high risks functions.

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

Appendix 1

Definitions

Audit Ratings

Satisfactory:
The control environment is considered appropriate and maintaining risks within acceptable parameters. There may be no or very few minor issues, but their number and severity relative to the size and scope of the operation, entity, or process audited indicate minimal concern.

Needs Minor Improvement:
The number and severity of issues relative to the size and scope of the operation, entity, or process being audited indicate some minor areas of weakness in the control environment that need to be addressed. Once the identified weaknesses are addressed, the control environment will be considered satisfactory.

Needs Improvement:
The audit raises questions regarding the appropriateness of the control environment and its ability to maintain risks within acceptable parameters. The control environment will require meaningful enhancement before it can be considered as fully satisfactory. The number and severity of issues relative to the size and scope of the operation, entity, or process being audited indicate some noteworthy areas of weakness.

Unsatisfactory:
The control environment is not considered appropriate, or the management of risks reviewed falls outside acceptable parameters, or both. The number and severity of issues relative to the size and scope of the operation, entity, or process being audited indicate pervasive, systemic, or individually serious weaknesses.

Appendix 2

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 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	• 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 • Any operational issue leading to injury of an employee or customer	• 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 2

Control Category	High	Medium	Low
	• Any operational issue leading to death 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 important compliance or regulatory impact	• 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 the above outcome
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 3

Distribution

Addressee(s) Hank McNeely, Director HR Information Management
Carrie Thomas, Director Total Rewards
Carlos Rodriguez, Director IT Security and Risk

Addressee(s) **Business Leaders:**
Barry Gilway, President/CEO/Executive Director
Violet Bloom, Chief Human Resource Officer
Kelly Booten, Chief Systems and Operations
Aditya Gavvala, VP IT Services and Delivery
Robert Sellers, VP Chief Technology Officer
Dan Sumner, Chief Legal Officer & General Counsel
Christine Turner Ashburn, Chief, Communications, Legislative & External Affairs
Mark Kagy, Acting Inspector General

Audit Committee:
Bette Brown, Citizens Audit Committee Chairperson
James Holton, Citizens Audit Committee Member
Senator John McKay, Citizens Audit Committee Member
Marc Dunbar, Citizens Audit Committee Member

Following Audit Committee Distribution:
The Honorable Rick Scott, Governor
The Honorable Jimmy Patronis, Chief Financial Officer
The Honorable Pam Bondi, Attorney General
The Honorable Adam Putnam, Commissioner of Agriculture
The Honorable Joe Negron, President of the Senate
The Honorable Richard Corcoran, Speaker of the House of Representatives

The External Auditor

Audit performed by Deena Harrison, Internal Audit Manager
Under the Direction of Joe Martins, Chief of Internal Audit