INTERNAL AUDIT

Centerpoint User Access (Financial and Procurement) Audit Report

February 27, 2019

Report Number: 2018-AUD-21 Centerpoint User Access (Financial and Procurement)

Table of Contents

Page

Executive Summary

Appendix

Executive Summary

Background

In 2016, Oracle Fusion Cloud Service, an integrated Enterprise Resource Planning (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 consisted of five phases with implementation dates ranging from April 2017 through November 2018. The Financial and Procurement modules within the Centerpoint application support three of the five phases, Accounting, Procurement, and Budgeting, which were implemented April 2017 through August 2018.

General ledger, accounts payable, fixed assets, cash management, and expense transactions are entered, processed, and managed in the Financial module. The Procurement module is utilized to enter, process, and manage purchase orders. Privileged roles within these modules allow assigned users the ability to create and modify financial transactions.

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 user access controls for the Centerpoint Financial and Procurement modules. 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 User Access for the Financial and Procurement modules is rated as **Needs Improvement.**

Results from our audit work indicate that Finance, Procurement, the Vendor Management Office, and the Centerpoint Project Team proactively collaborated to design and implement appropriate user access controls. However, system limitations and the complexity of Oracle roles and permissions contributed to challenges in effectively managing user access across all Centerpoint modules. In addition, guidance from the vendor procured to assist with implementation influenced Citizens' initial decisions surrounding user role customization and enabling audit functionality. As Citizens gains more knowledge and experience with Centerpoint, management has acknowledged the need to re-evaluate certain decisions made during implementation including user access design for all modules.

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

- **Roles and permissions are not clearly defined resulting in instances of inadequate segregation of duties and excessive permissions that are not adequately monitored.** Individuals are assigned to conflicting roles within the Financial and Procurement modules 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 and initial user role design decisions made based on guidance from the vendor procured to assist during implementation. 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.

- **Monitoring and oversight of the provisioning process does not include a comprehensive review of auto-provisioning and external users including suppliers.** Our work revealed a small number internal and external users for which documentation was not readily available to confirm the identity of the users and/or the appropriateness of the roles assigned. Internal Audit together with IT management performed additional research to validate these users and roles resulting in the identification of manual errors and system limitations that were not previously detected by the existing monitoring processes. Failure to adequately monitor user provisioning may result in misuse and misappropriation of company information technology resources, resulting in potential business interruption or financial loss. IT and management have initiated actions to correct roles and user access as appropriate.

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 that will continue to have access to sensitive and high risks functions. In addition, management should consider conducting further testing on the end-to-end external supplier registration process prior to enabling any new supplier functionality.

Internal Audit provided management with a detailed matrix of identified potential incompatible segregation of duties based on the current role design to assist with addressing user specific concerns and any role redesign efforts.

Executive Summary

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) Andrew Woodward, Senior Director Controller
Diane Walker, Director IT Operations
Spencer Kraemer, Director Purchasing
Stephen Guth, Vice President – Vendor Management

Addressee(s) **Business Leaders:**
Barry Gilway, President/CEO/Executive Director
Jennifer Montero, Chief Financial 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
Matt Gerrell, Director – Accounting & Budget
Jonathan Evans, Supervisor Service Assurance

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 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 Deena Harrison and Mike Walton, Internal Audit Managers
Under the Direction of Joe Martins, Chief of Internal Audit