AX ERP System - Segregation of Duties Audit (18-05)

Terry Follmer, VP of Internal Audit

Distribution List:
Capital Metro Board of Directors
Randy Clark, President and CEO
Elaine Timbes, Deputy Chief Executive Officer and Chief Operating Officer
Kerri Butcher, EVP, Chief Counsel & Chief of Staff
Donna Simmons, EVP Administration, Safety, Risk Management & EEO
Todd Hemingson, EVP, Strategic Planning & Development
Reinet Marneweck, EVP, Chief Financial Officer
Dottie Watkins, VP, Bus Operations
David Deck, VP, Rail Operations
Ken Cartwright, VP, Capital Projects
Joe Iannello, VP, Chief Information Officer
Shanea Davis, VP, Real Estate, Property & Asset Management
Chad Ballentine, VP, Paratransit & Innovative Mobility Solutions
Brian Carter, VP, Marketing and Communications
Gardner Tabon, VP, Risk, Safety, and Accessibility
Muhammad Abdullah, Director Procurement
Lea Sandoz, Controller
Rafael Villarreal Jr., Director of Contract Oversight – Bus and Paratransit Services

Executive Summary

As part of our FY2017–2018 Audit Plan approved by the Capital Metro Board, we completed an audit of user access and segregation of duties within the Capital Metro Microsoft Dynamics AX ERP System. The audit results including the objective, scope, and conclusion are as follows.

Background

In October 2015, the Microsoft Dynamics AX system replaced Oracle as the Financial Enterprise Resource Planning (ERP) system for Capital Metro. The implementation of AX provided the following functionality: General Ledger, Accounts Payable, Fixed Asset, Purchasing, Accounts Receivable, Budgeting, Planning and others. This AX system provides for workflow and approval of transactions for more than 200 users in various departments (e.g. Accounting, Procurement, Bus and Rail Operations, Human Resources, etc.).

In order to perform the analysis of user access, security and segregation of duties, Fastpath GRC Studio was implemented on January 12, 2018. This tool provides the following two capabilities: 1) Logging System: Log activities occurring within AX core application, the enhancement and customizations implemented, and any 3rd party vendor software integrated with AX and activities within all databased that AX uses, and 2) Segregation of Duties (SOD) System: Provide a Segregation of Duties evaluation, analysis, correction and monitoring system.

Audit Objective & Scope

The primary objective of the audit was to review the SOD and related controls in the AX ERP system with a focus on reviewing 1) user access conflicts and 2) required monitoring and logging for the SOD conflicts. The scope included attending meetings with management to review identified risk in the Fastpath System, review user access assigned in the AX ERP System, conduct interviews of staff members from IT, Finance, and Procurement, and perform activities in the test environment system of the AX ERP system for the following modules Accounts Payable, Accounts Receivable, General Ledger and Procurement and Sourcing. The testing period of the audit covers from February 2018 through July 2018.

Opinion

Internal controls are generally in place and properly functioning related to the segregation of duties for the AX ERP System. Management has been developing SOX-like narratives to document internal controls and compliance testing program is being developed. In our opinion, internal controls require improvement in the following areas: monitoring and tracking of IT vendor system administrator usage on AX system; logging and monitoring of SOD conflicts; and optimizing user access profiles that are assigned to users.

This audit was conducted in accordance with US Government Accountability Office's Generally Accepted Government Auditing Standards (GAGAS) and the Institute of Internal Auditor's International Standards for the Professional Practice of Internal Auditing. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The audit was conducted by the following staff members in the Capital Metro Internal Audit Department:

- Jeannette Lepe, Internal Auditor II
- Terry Follmer, VP Internal Audit

Recommendation to strengthen controls and improve accountability were provided to management. Management concurs with the results of our work and has provided management action plans which are included in the table below. A follow-up audit is performed semi-annually (i.e. May and November) to ensure management action plans for all issued audit reports are completed timely.

We appreciate the cooperation and assistance provided to us throughout this audit.

NO. ISSUE & RISK	RECOMMENDATION	MANAGEMENT ACTON PLAN
1. VENDOR SYSTEM ADMINSTRATOR USAGE ON SYSTEM An IT vendor has been contracted to provide system support and training on the implementation and troubleshooting to support the AX ERP System. We noted that they have System Administrator rights to the Production Environment and this access is not being removed timely or consistently monitored.	Management should only provide System Administrator rights when needed, and this access should be removed once maintenance is performed. Additionally, logging and monitoring of System Administrator accounts should be in place for all accounts.	IT will create a Service Now ticket when providing IT Contractor Staff the System Administrator role. The ticket shall remain open until the role is removed. **Target Completion Date**: 08/01/2018
2. LOGGING & MONITORING OF SOD CONFLICTS Management was able to identify and mitigate most of the segregation of duties conflicts using the Fastpath tool. Due to the small size of the Accounting Department and the need to have a backup when staff is out of the office, some SOD Conflicts listed as High and Medium have been determined to be impractical to make further segregation of duties. We noted that logging and monitoring of these accounts with SOD conflicts is not in place. Errors and irregularities may not be detected timely without compensating controls for the SOD conflicts.	Management should consider defining and implementing the necessary logging and periodic monitoring of user access to ensure that compensating controls are present to detect inappropriate transactions due to limited segregation of duties.	Controller will define and implement monitoring of SOD conflicts based on the developed list. **Target Completion Date**: 08/15/2018

NO.	ISSUE & RISK	RECOMMENDATION	MANAGEMENT ACTON PLAN
	3. <u>OPTIMIZING USER ACCESS PROFILES & DESCRIPTIONS</u> The AX ERP system allows for custom roles to be developed and assigned to users, and one user can be assigned multiple/many roles. This situation can result in "role creep" whereby a single user may have many role templates assigned to them resulting in unnecessary and inappropriate transactional capabilities. We reviewed a sample of users to determine what roles and capabilities have been provided and noted the following: • The Accounting Manager has both the accounting supervisor and the accounting manager roles assigned, making analysis of individual user capabilities more difficult to understand and manage. Having a single customized role assigned will provide more clear visibility as to user capabilities to perform transactions. • The "Setup" option in AX is an Administrator capability that allows a user to establish and edit menu preferences in the AX system, including changes to workflows. We noted some users who should not be assigned "Setup", which allows them to make changes to AP workflow process, parameters, and vendor accounts. • The AX "role descriptions" provided by AX as well as some of the new descriptions created by Capital Metro do not accurately describe the capabilities of the roles assigned, which may result in unnecessary and inappropriate access being assigned.	Management should consider making the following improvements to user access and security controls: • Review users who have been assigned multiple roles and consider developing a single custom role that reflects only the need to know and need to do within the system. • Review all users and roles that have the "setup" capability and limit this access based upon a need to know and need to do. • Consider renaming descriptions that do not accurately reflect users capabilities in the AX system, which will help in the analysis and administration of system access.	IT will review and limit access on roles as deemed appropriate as directed by the Controller. Descriptions of roles will be updated to accurately reflect roles. **<u>Target Completion Date</u>**: 4/30/2019