COUNTY OF EL PASO

OFFICE OF THE COUNTY AUDITOR

EDWARD A. DION, CPA
COUNTY AUDITOR
edion@epcounty.com
www.epcounty.com/auditor

County Administrative Offices
800 East Overland Street, Rm. 406
EL PASO, TEXAS 79901-2407
(915) 546-2040
(915) 546-8172 FAX

07-11

July 15, 2020

Mr. Esteban Fernandez
Audit Manager Senior
Auditor's Office
800 E. Overland, Rm 406
El Paso, Texas 79901

Dear Mr. Fernandez:

The County Auditor's Internal Audit division performed an audit of the County's financial system and procedures of the System Administration and Support division of the County Auditor's Office to determine if internal controls are adequate to ensure proper administration over user access control. Policies, procedures, and regulations were also reviewed to ensure processes are documented, operating and efficient.

The audit report is attached. We tested seven operating controls with a total of 1,569 samples. There were eight findings noted as a result of the audit procedures. We wish to thank the management and staff of the System Administration and Support division for their assistance and courtesies extended during this audit.

Because of certain statutory duties required of the County Auditor, this office is not independent in regard to your office, as defined by AICPA professional standards. However, our audit was performed with objectivity and due professional care.

Respectfully,

Edward A. Dion
County Auditor

EAD:ML:ya

cc: Mr. Victor Perez, Financial Operations Director

EXECUTIVE SUMMARY

BACKGROUND

On October 1, 2016, El Paso County transitioned from various legacy systems to the Munis Enterprise Resource Planning (ERP) system. The County implemented a three year phased changeover with the financials and work order modules going live in October 2016, the human resources and payroll modules in October 2017, and additional reporting modules in April 2018. The Munis ERP system combined multiple County processes into one integrated system to improve operations and efficiencies among County departments. During and post implementation, the Information Technology Department (ITD) managed user access controls. However, responsibility for access controls was transferred to the County Auditor's Financial System Maintenance and Support division (System Administration) in May 2019. This audit was performed by Michael Lamas, IT auditor - senior. This is the first internal audit of Munis Access Controls.

The design and assignment of job and data roles are key components of user controls for Munis system security. A Munis job role is a set of permissions assigned to a user to grant them access to perform actions within Munis programs. A Munis data role is a set of permissions assigned to a user to grant them access to data within Munis programs. Together, job and data roles grant Munis users access to the information and programs they need to perform their day to day operations.

SCOPE

The scope of the audit includes user roles and assignments from October 2016 through October 2019.

AUDIT OBJECTIVES

The audit evaluated the adequacy of access controls, roles, user assignments, and user accounts within the Munis ERP system. Following are the business objectives and related control assessment.

Business Objective	Control Assessment
1. Current end user roles are designed and operating in an effective manner	Needs Improvement
2. Current end user assignments are designed and operating in an effective manner	Needs Improvement
3. System administrator roles are designed and operating in an effective manner	Needs Improvement
4. Role creation and modification has required supporting documentation	Needs Improvement
5. Munis user accounts are reviewed and maintained to limit stale user accounts	Unsatisfactory
6. County Auditor management review of changes implemented by System Administration	Unsatisfactory
7. System Administration staff follows written policies and procedures	Needs Improvement

METHODOLOGY

To achieve the audit objectives we:

- Reviewed all Munis job and data roles.
- Reviewed all end user role and menu assignments.
- Reviewed all system administration roles and user accounts.
- Tested a sample of changes made to user accounts and roles for adequate supporting documentation.
- Reviewed all Munis user accounts to determine the number of inactive or stale accounts.
- Evaluated reports available to County Auditor management and examined any review procedures performed by management.
- Interviewed System Administration management to evaluate unwritten policies and procedures.

EXECUTIVE SUMMARY

RESULTS

Listed below are controls and findings summaries, with findings listed from highest to lowest risk. Please see the *Findings and Action Plans* section of this report for details and management action plans.

Control Summary	
Good Controls	**Weak Controls**
	• End user role design and operation (Obj. 1) • End user assignment design and operation (Obj. 2) • Administrative role design and operation (Obj. 3) • Role changes with supporting documentation (Obj. 4) • Stale account management (Obj. 5) • Auditor management change review (Obj. 6) • Documentation of policies and procedures (Obj. 7)

Findings Summary

1. High risk end user roles in the Human Resources (HR) department lack adequate access controls.
2. The County Auditor GL and Disbursement Reporting Audit (GLDRA) division lacks adequate access controls.
3. Munis administrator role in use by ITD and System Administration staff.
4. There is a lack of adequate management review of access control changes.
5. There is a lack of adequate documentation for access control changes.
6. Role creation and maintenance does not follow role based access control (RBAC) standards.
7. There is no policy on inactivating stale users.
8. Policies and procedures need to be documented.

INHERENT LIMITATIONS

This operational review was designed to provide reasonable assurance that the internal control structure is adequate to safeguard the County's assets from loss, theft, or misuse. The County's internal control structure is designed to provide reasonable, but not absolute assurance that these objectives are met. The concept of reasonable assurance recognizes that: (1) the cost of implementing the controls should not exceed the benefits likely to be derived; and (2) the valuation of costs and benefits requires the use of estimates and judgment by management. Because of the inherent limitations in any system of internal controls, errors or irregularities may occur and not be detected.

CONCLUSION

The System Administration division has maintained access controls over the Munis application on an ad hoc basis with little documentation and lacks written policies and procedures; however, the division has recently implemented improvements regarding the maintenance of proper change documentation and the documentation of policies and procedures. All seven identified business objectives need improvement. Implementing the recommendations in this report should improve access control management.

FINDINGS AND ACTION PLANS

Current Audit Findings and Action Plans

Finding #1	Risk Level (H)

Human Resources Access Controls – All HR users were found to have unrestricted access to the human resources and payroll modules within Munis. Roles with elevated access were granted to HR users during the implementation phase of the Munis ERP system but were never removed.

Data security best practice and El Paso County IT policy related to the principle of least privilege states users should only have access to permissions and information which are essential for the employee to perform their intended function. The current unrestricted user access puts the County at high risk of employee data leakage, litigation resulting from data leakage, creation of fictitious employees, and unauthorized manipulation of current employee data. This access also poses high risk to data security if any user credentials are compromised.

Recommendation

System Administration management should immediately remove HR access to payroll setup and processing. Additionally, System Administration should coordinate with the HR department to review existing HR jobs and create new roles that follow the principle of least privilege. Mass employee data extraction rights should be granted to personnel on an as needed basis and data extracted should be secured according to data privacy laws and data security best practices such as password protection and encryption.

Action Plan

Person Responsible	System Administration Manager Senior	Estimated Completion Date	9/15/2020

System Administration and County Auditor management will meet with HR department management to discuss suggested changes to HR roles. Esteban will set up an action plan and work with the HR department to ensure successful deployment of the new roles.

Finding #2	Risk Level (H)

GL and Disbursement Reporting Audit Division Access Controls – Roles assigned to GLDRA users contain permissions which allow staff to complete the payment process without proper approvals or review. These roles were assigned to users following legacy financial system processes and these processes were not reviewed post-implementation.

El Paso County IT policy related to the principle of least privilege requires users only have access to privileges which are essential for a user to perform their intended function. The current roles allow staff to create or modify vendors, create invoices, and cut checks without any workflow or review.

Recommendation

GLDRA and System Administration should review current departmental procedures and separate job duties to allow for proper payment processing workflow and review. New roles should be created to facilitate assigned duties only and current roles should be inactivated.

Action Plan

Person Responsible	GL&DRA Audit Manager Senior	Estimated Completion Date	3/1/2020

A concurrent review by Internal Audit of vendor master file access controls found the same control weaknesses and as such, the Auditor's department has already implemented changes to improve the risk management over

the GLDRA division. It is expected that the issues identified in the current audit have been addressed and the adequacy of these changes will be reviewed during the next audit.

Finding #3	**Risk Level** H

Administrator Accounts –The Munis administrator role was used by ITD and System Administration users during implementation in order to expedite configuration; however, assignment of this role was not reevaluated post-implementation. The Munis administrator role is currently assigned to two System Administration users and seven ITD users. Administrator accounts are user accounts with full privileges on a computer system. In the Munis application, the administrator account allows a user to view all data, perform all user functions, and execute system maintenance and update processes. Use of these accounts should be limited to users performing critical system functions and should only be used on an as needed basis.

El Paso County IT policy and data security best practice requires limiting the use of administrator accounts. The use of administrator accounts increases the overall risk to the Munis system by allowing users to quickly override any implemented access controls and delete some audit trails. Additionally, the elevated privileges granted by the administrator role pose a high risk to data security if any user credentials are compromised.

Recommendation

System Administration staff should review System Administration and ITD job duties and responsibilities and create new roles for both departments. These new roles should then be presented to Auditor and ITD executive management in order to ensure the new roles are correctly designed and implemented. Users in both departments should only have inquiry access to non-system administration programs. System Administration should limit any testing and troubleshooting that requires administrator rights to the train and test environments in order to protect the integrity of the live data environment.

Action Plan

Person Responsible	**System Administration Manager Senior**	**Estimated Completion Date**	**8/15/2020**

System Administration will meet with ITD to determine what Munis access is appropriate for each department. Use of the Munis role will be discontinued and System Administration will create new administrative roles both departments.

Finding #4	**Risk Level** M

Management Review and Reporting – Auditor executive management does not receive any reports nor do they have the ability to independently run reports related to Munis access controls and System Administration activity. Auditor management was not trained on reporting or auditing the access control process when the responsibility over this function was fully transferred to the County Auditor.

Best practices recommend monitoring whenever hard controls are not available. Inadequate review increases the risk that unapproved changes are implemented in the system, erroneous data is entered into the system, or implemented access controls are overridden.

Recommendation

Management needs to be able to run reports in order to obtain independent confirmation of the validity of the changes and data entered by System Administration. Management should review changes in role permissions and assignments, the integrity and completeness of system audit trails, and the validity of any journals or other financial

data entered by System Administration staff. Auditor recommends reviewing reports on a weekly basis due to the large volume of data generated by role changes and audit logs.

Action Plan			
Person Responsible	**System Administration Manager Senior**	**Estimated Completion Date**	**7/15/2020**

System Administration will meet with County Auditor management to develop reports and train on using those reports to review changes implemented by the System Administration department. Independent management review will occur on a weekly basis with Auditor management rotating review duties each week.

Finding #5 **Risk Level** M

Supporting Documentation – System Administration does not keep adequate documentation for all access control changes. In a sample of 30 items, 19 or 63% of changes to roles or user assignments are documented. An additional 6 or 20% were initiated by System Administration users as part of their role maintenance process and an explanation was provided. In total, 25 or 83% of sampled items were adequately documented and 17% lacked documentation. System Administration staff does not maintain all backup in a centralized location and instead relies on several filing systems.

Adequate documentation is essential whenever an implemented change needs to be validated by management. The lack of documentation increases the risk that an unauthorized access control change is implemented and that this change is not discovered upon management review.

Recommendation

System Administration staff should maintain proper documentation for all access control changes in a centralized location.

Action Plan			
Person Responsible	**System Administration Manager Senior**	**Estimated Completion Date**	**4/1/2020**

System Administration has designated a centralized location for all backup and will now require backup for all changes. Additionally, the division will now send out an email to any affected employee when performing maintenance on Munis roles. The adequacy of the new backup procedures will be reviewed during the next audit.

Finding #6 **Risk Level** M

Role Standardization – Munis roles do not follow a consistent set of standards. For example, some roles are based on vendor recommended RBAC principles while others are based on user specific needs. The sample for this review consisted of the full population of 326 job and 177 data roles. 308 or 95% of job roles have a data element and 133 or 75% of data roles have a job element. As per an interview with System Administration management, the absence of consistent standards among stakeholders as well as the lack of prior experience with RBAC based systems contributed to the identified issues.

Commingling job and data attributes goes against vendor recommendations and, combined with the lack of standardization, further increases the size and complexity of the role management system, which increases the risk of diminished or compromised system controls.

Recommendation
System Administration management should organize job duties and responsibilities into functions and recreate roles based on RBAC standards instead of maintaining a user or job based system. The division should assign these roles to users and gradually phase out the old roles.

Action Plan			
Person Responsible	**System Administration Manager Senior**	**Estimated Completion Date**	**10/1/2020**
System Administration will meet with the IT Department in order to review the steps taken when designing roles as part of implementation process. The System Administration division will then work to create a long term plan to review all roles in order to better follow RBAC guidelines. This will be a long term project and progress will be evaluated during the next audit period.			

Finding #7 **Risk Level** L

Stale Accounts – System Administration does not have a stale user account policy, as such, the division does not perform an active user review to limit the number of stale users in the system.

Account management best practices dictate that user accounts be deactivated after a predefined period of inactivity. Stale accounts can be used by unauthorized individuals to access sensitive information, process fraudulent transactions, and delete data. The presence of stale user accounts in the Munis system increases the risk of unauthorized access to the system if credentials are compromised.

Recommendation
System Administration staff should deactivate Munis application accounts even if ITD has a policy to deactivate system-wide user accounts. Deactivating these accounts on the application level provides a second layer of defense against unauthorized use and ensures that the number of active accounts remains within a manageable range.

Action Plan			
Person Responsible	**System Administration Manager Senior**	**Estimated Completion Date**	**9/30/2020**
System Administration will develop a stale account policy as part of their policies and procedures. Stale account policy will be presented to Auditor management for approval.			

Finding #8 **Risk Level** L

Policies and Procedures – System Administration currently operates on an unwritten set of policies and procedures. Policies and procedures were not documented after full responsibility over the access control function was assumed.

As per COBIT[1] objective APO1.09, management should put in place policies and procedures to maintain compliance, measure performance, and improve future controls. The lack of written policies and procedures increases the risk that System Administration staff will perform their duties in an inconsistent manner.

[1]COBIT is an IT management framework to help businesses develop, organize and implement strategies around information management and governance.

FINDINGS AND ACTION PLANS

Recommendation			
System Administration should document policies and procedures for the division.			
Action Plan			
Person Responsible	**System Administration Manager Senior**	**Estimated Completion Date**	**9/30/2020**
System Administration is working with the policy auditor to develop written policies and procedures. The new policies and procedures are expected to address many of the issues identified in the audit.			