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

04-16 April 12, 2023

Mr. Esteban Fernandez
Audit Manager Senior
County 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 related policies 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 workflow access control. Policies, procedures, and regulations were also reviewed to ensure processes are documented, operating and efficient.

The audit report is attached. We tested four operating controls with a total of 240 samples. There were five 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 division of the County Auditor's 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: The Honorable Anna Perez, Administrative District Judge, 41st District Court
Mrs. Barbara Parker, County Auditor First Assistant
Mr. Victor Perez, Financial Operations Director

Munis Workflow Audit
For the Period of June 2021 through June 2022

EXECUTIVE SUMMARY

BACKGROUND

The Munis Enterprise Resource Planning (ERP) system has been in use by most of the County of El Paso for the past six and a half years. Prior to the adoption of the ERP system, workflow relied on manual authorization and controls. The workflow approval process was highly decentralized and workflow audit records were maintained through a variety of physical and electronic means. After the adoption of the ERP system, the process was centralized, and most departmental approval transactions transitioned to an automated electronic system. Since May 2019, System workflow has been managed by the County Auditor's Financial System Maintenance and Support division (System Administration). Prior to May 2019, the Information Technology Department (ITD) was responsible for managing this function. For further information on this topic see OP-18-594, copy attached. The County Auditor has increased focus on information technology audits due to the risks associated with the transition from a manual to an electronic financial records system. This emphasis on the IT internal audit activity provides assurance that internal controls are adequate to mitigate risk, governance processes are effective, and organizational objectives are met. This audit was performed by Michael Lamas, IT auditor - senior. This is the first internal audit of ERP System Workflow.

The ERP application utilizes the Workflow Business Rules (WBR) program to manage approval and notification routing for most programs. The available rules set depends on the type of transaction and program. For example, a financial approval may have the option to route workflow depending on department, location, amount, or financial account while a personnel management approval may be routed only through location or department. Additionally, some departments still utilize physical approvals such as wet signatures. However, physical documents are still uploaded to the Munis system to maintain a complete electronic approval record.

The audit of the WBR program utilizes the COBIT 2019 control framework and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. COBIT is an IT management framework created by the Information Systems Audit and Control Association to help businesses develop, organize, and implement strategies around information management and governance. NIST SP 800-53 provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations from a diverse set of threats and risks. NIST is a federal agency tasked with developing cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies, and the broader public. COBIT 2019 references herein are designed to work with the NIST Cybersecurity Framework, whose controls are mapped out in NIST SP 800-53.

SCOPE

The scope of the audit includes user roles and assignments from June 2021 through June 2022.

AUDIT OBJECTIVES

The audit evaluated the adequacy of the WBR and the approvals process within the Munis ERP system.
Following are the business objectives and related control assessment.

Business Objective	Control Assessment
1. Current WBR are designed and operating in an effective manner	Needs Improvement
2. WBR change control processes are well designed, documented, and operating in an effective manner	Unsatisfactory
3. WBR are regularly reviewed and tested for operating effectiveness	Needs Improvement
4. System Support and Administration staff follow written policies and procedures	Unsatisfactory

EXECUTIVE SUMMARY

METHODOLOGY

To achieve the audit objectives, we:

- Tested a stratified sample of ERP WBR.
- Tested a stratified sample of approval actions.
- Tested a sample of changes made to WBR for adequate supporting documentation.
- Interviewed System Administration management to determine unwritten policies and procedures.
- Interviewed ITD and Human Resources (HR) staff to determine written and unwritten policies and procedures.

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.

<table>
<tr><th colspan="2">Control Summary</th></tr>
<tr><th>Good Controls</th><th>Weak Controls</th></tr>
<tr><td></td><td>• Workflow business rule design and operation (Obj. 1)
• Workflow business rule change control process design, documentation, and operation (Obj. 2)
• Regular review of WBR (Obj. 3)
• Adherence to written policies and procedures (Obj. 4)</td></tr>
<tr><th colspan="2">Findings Summary</th></tr>
<tr><td colspan="2">1. The personnel management workflow process lacks separation of duties, dual authorization, and proper written documentation.
2. Some purchasing workflow processes lack separation of duties or dual authorization.
3. There is a lack of adequate review of workflow changes.
4. There is a lack of adequate documentation for workflow changes.
5. Policies and procedures need to be documented, including critical workflow paths.</td></tr>
</table>

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 controls over the Munis WBR application on an ad hoc basis with little documentation and lacks written policies and procedures. Two identified business objectives need improvement and two are deemed unsatisfactory. Implementing the recommendations in this report should improve workflow management oversight and control by the Auditor's office. Additionally, this will require greater collaboration with departments requiring limiting employee access to only what is necessary for each job rather than granting greater authority and access resulting in incompatible functions and unnecessary risk to the County.

FINDINGS AND ACTION PLANS

Current Audit Findings and Action Plans

Finding #1 — Risk Level H

Personnel Management Workflow Controls – All personnel management workflow processes contain multiple individuals from multiple HR divisions regardless of purpose. In a sample of 45 transactions, 19 transactions (42%) contained duplicate HR workflow approval steps. Two transactions (4%) were entered and approved by the same individual and 3 transactions (7%) contained no supporting documentation. Auditor interviewed the HR Recruitment Division Manager, System Administration Audit Manager Senior, and ITD Division Manager to determine the rationale for workflow approver assignments in the HR department. As per the interviews, the HR department values cross training and routinely moves staff from one division to the other. Due to this, it is easier for the workflow approval process to remain open to most permanent and temporary staff. Interviewed management was unable to determine why there is an additional, duplicate step in some workflow approvals.

NIST 800-53 AC-6, Least Privilege, states organizations should allow only authorized access for users that is necessary to accomplish assigned organizational tasks. As per HR Recruitment Division Manager, HR departmental policies and procedures dictate that no user should approve their own transactions and all workflows should have supporting documentation. The current personnel management workflow process lacks consistency and could pose a security risk if erroneous transactions are entered into the system due to the lack of effective workflow controls.

Recommendation

System Administration management should collaborate with HR management to determine how to accomplish personnel management workflow efficiently and securely. The auditor recommends removing all non-essential staff from workflow approval and performing training functions in the training environments. Preferably, temporary access to the production environment should only be granted to fully trained or properly supervised staff. The Auditor and HR departments should review all personnel management workflow and remove any duplicate steps.

Action Plan

Person Responsible	**System Administration Manager Senior**	**Estimated Completion Date**	**9/30/2023**

System Administration management will coordinate a meeting with HR to discuss duplicate workflow and auditor's recommendations. HR, custodian of the personnel management module, will be requested to document essential workflow authority and approval levels in order to implement auditor recommendations and address existing risks. System Support will follow HR direction and change workflow permissions accordingly.

Finding #2 — Risk Level H

Requisitions and Purchasing Workflow Controls – Requisition and purchasing workflow processes in the ERP system do not enforce dual review of purchasing transactions. In a sample of 45 transactions, 11 sampled items (24%) do not have supervisory review and were ordered and received by the same employee. Additionally, one item (2%) also does not have proper review but was received by a separate employee. Requisition approval workflow must be set up for each department; otherwise, the default requisition entry role (JOB_REQ/PO_CLERK) allows users to enter and release their own requisitions as well as receive items. Therefore, the process relies on workflow management to ensure requisitions are reviewed by a secondary employee before release to the Auditor's Department.

NIST 800-53 AC-5, Separation of Duties, recommends dividing business functions among different individuals or roles to reduce the risk of malevolent activity without collusion. Additionally, NIST 800-53 AC-3(2) recommends utilizing a dual authorization mechanism to reduce the risk of insider threat. The lack of separation of duties and dual authorization within the current roles and workflow process can lead to unnecessary purchases or the misappropriation of assets for personal use.

Recommendation

System Administration should review current workflow assignments and coordinate with the Purchasing department to ensure all departments have secondary purchase review. The workflow process should be discussed, with risks documented and approved by the affected department whenever secondary approval roles are declined by management.

Action Plan

Person Responsible	**System Administration Manager Senior**	**Estimated Completion Date**	**9/30/2023**

System Administration management will coordinate a meeting with the Purchasing department to discuss auditor's recommendations. Purchasing, custodian of the requisitions and purchasing module, will determine whether to implement recommendations or accept risk. System Support will coordinate with relevant departments to issue new countywide purchasing recommendations if deemed appropriate by the Purchasing department.

Finding #3 **Risk Level** M

Workflow Configuration Review – There is no documented and systematic review of changes to the workflow process. Most changes are currently entered into the live environment of the Munis system and are not approved by a secondary reviewer before deployment. Additionally, there is no scheduled post implementation review of any workflow changes.

As per COBIT BAI06.01, Evaluate, Prioritize and Authorize Change Requests, management should evaluate all requests for change to determine the impact and assess whether change will adversely affect the operational environment and introduce unacceptable risk. NIST 800-53 CM-3, Configuration Change Control, recommends the pre-deployment review and documentation of all change decisions associated with the system as well as additional monitor and review activities once the changes are implemented. The lack of a documented workflow configuration process increases the risk that unapproved or erroneous changes are implemented in the system.

Recommendation

System Administration staff should implement a workflow configuration change review process. All changes should be reviewed by a separate System Administration staff member before deployment. Additionally, new or complex workflow changes should be tested in the training environment before deployment to the live environment.

Action Plan

Person Responsible	**System Administration Manager Senior**	**Estimated Completion Date**	**6/30/2023**

The System Administration division will create policies and procedures for the update and creation of WBR. A manual log or some other recording system will be maintained for all workflow changes.

Finding #4 — Risk Level M

Workflow Configuration Change Documentation – The System Support division does not keep adequate supporting documentation for all workflow configuration changes. In a sample of 15 workflow changes, 6 sampled items (40%) do not have formal change forms and are instead either email or teams message requests. Two sampled items (13%) do not have any written documentation.

As per COBIT BAI06.03, Track and Report Change Status, management should maintain a tracking and reporting system to document changes and ensure that approved changes are implemented as planned. Additionally, as per COBIT BAI06.04, Close and Document Changes, whenever changes to an application are implemented, management should update documentation and procedures affected by the change.

Recommendation

System Administration should ensure all workflow changes are documented, preferably using the formal change form approved by ITD. If no formal change form is available, the request should at least be received through a written document. Furthermore, change documentation should be saved in a secure and easily accessible location. Comments related to the solution for the change request should be added to the received form since there is no commenting function in the Munis workflow system.

Action Plan

Person Responsible	**System Administration Manager Senior**	**Estimated Completion Date**	**6/30/2023**

The System Administration division will create policies and procedures for WBR change documentation. The division will ask for modifications to the ITD change form or create an internal change form to better document WBR changes.

Finding #5 — Risk Level M

Policies and Procedures – System Administration does not have written policies and procedures for the workflow administration process. The staff currently responds to requests on a case-by-case basis in an ad hoc manner. The division maintains no documentation/mappings of critical workflow paths.

NIST 800-53 AC-1, Policies and Procedures, recommends the adoption of organization, mission, and business level policies and procedures. The lack of written policies and procedures increases the likelihood of errors and increases key person dependency risk.

Recommendation

System Administration staff should review the workflow process, develop and maintain written policies and procedures. If possible, the division should consult with ITD to ensure the policies are aligned with county wide cybersecurity and access control policies. Specific procedures and critical workflow mapping should be created and maintained.

Action Plan

Person Responsible	**System Administration Manager Senior**	**Estimated Completion Date**	**6/30/2023**

The division will create written policies and procedures for the WBR process. Management will consult with ITD to ensure their policies align with county wide access control policies.