# 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

06-03

June 7, 2022

Mr. Chris Stathis
Information Technology Department
800 E. Overland, Suite 400
El Paso, Texas 79901

Dear Mr. Stathis:

The County Auditor's Internal Audit division performed an audit of the County's courts and justice management system (Enterprise Justice (Odyssey)) access 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 six operating controls with a total of 952 samples. There were six findings noted as a result of the audit procedures. We wish to thank the management and staff of the ITD - Enterprise Software 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: Mrs. Betsy Keller, Chief Administrator
Mr. Carlos A. Puga, IT Division Manager - Software
Mr. Ric Rocha, Enterprise Software Supervisor (Courts & Justice)

# EXECUTIVE SUMMARY

## BACKGROUND

Beginning in 2011, El Paso County began a transition from various legacy systems to the Odyssey Courts and Justice Management system (Enterprise Justice). The County implemented a phased changeover starting with Civil Case Modules in August 2011, Criminal Case Modules in August 2013, and several, smaller modules after October 2015. Enterprise Justice combined multiple processes into one integrated system to improve operations and efficiencies in the courts. The design and assignment of job and data roles are key components of user controls for Enterprise Justice system security. A role is a set of permissions assigned to a user to grant them access to perform actions and access data within Enterprise Justice programs. Roles are assigned to users depending on the permissions required to perform their essential job functions.

The Information Technology Department (ITD) is headed by the Chief Information Officer, the Deputy Chief Information Officer, and the Chief Information Security Officer. The department is organized into the Administration, Software, Projects, Infrastructure, and Support Divisions. These divisions are further subdivided into teams dedicated to managing different aspects of the County's information technology infrastructure. Enterprise Justice is managed by the Courts & Justice group within the Enterprise Software Division. Six software specialists and four help desk team members currently have access control rights in the Enterprise Justice software. The division reports to the Deputy Chief Information Officer. This audit was performed by Michael Lamas, IT auditor - senior. This is the first internal audit of Enterprise Justice access controls.

## SCOPE

The scope of the audit includes user roles and assignments from July 2020 through July 2021.

## AUDIT OBJECTIVES

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

| Business Objective | Control Assessment |
|---|---|
| 1. Policies and procedures related to access controls are documented, reviewed, and operating in an effective manner | Unsatisfactory |
| 2. Administrative roles are designed and operating in an effective manner | Needs Improvement |
| 3. User assignments are designed and operating in an effective manner | Needs Improvement |
| 4. Role creation and modification has required supporting documentation | Unsatisfactory |
| 5. Stale user accounts are routinely reviewed and managed according to policy | Unsatisfactory |
| 6. Supervisory staff or management reviews changes made to permissions and access controls | Unsatisfactory |

## METHODOLOGY

To achieve the audit objectives, we:

- Reviewed all Enterprise Justice roles.
- Reviewed all administration roles and user accounts with administrative permissions.
- Reviewed available access control audit reports and change logs.
- Reviewed all accounts to determine the number of stale accounts.
- Examined any review procedures performed by management.
- Interviewed the Enterprise Software Supervisor (Courts & Justice) 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** |
| | • Administrative role design and operation (Obj. 2)<br>• User assignment design and operation (Obj. 3)<br>• Role changes with supporting documentation (Obj. 4)<br>• Stale account management (Obj. 5)<br>• Management change review (Obj. 6)<br>• Documentation of policies and procedures (Obj. 1) |

**Findings Summary**

1. Inadequate administrative role design and duplicate permissions.
2. Assignment of administrative roles to multiple users outside of the Courts and Justice Software Management Team.
3. Lack of adequate documentation for access control changes.
4. Stale users are not inactivated as per departmental policy.
5. Management does not review changes made by the Courts and Justice Software Management Team.
6. 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 ITD Courts & Justice group has maintained access controls over the Enterprise Justice application on an ad hoc basis with little documentation and a lack of written policies and procedures. However, the division has recently implemented improvements regarding the maintenance of proper change documentation. All six identified business objectives need improvement with special consideration given to the review of current role permissions and the implementation of a software-based audit trail. 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

**Administrative Role Design and Operation** – Certain roles within the Enterprise Justice application have been set up with increased administrative rights. These rights include the ability to create, delete, and modify users and roles as well as assign roles to users. Use of these accounts should be limited to users performing critical system functions and should only be used on an as needed basis. User role analysis determined the following:

| User Role Determination | Role Count |
|---|---|
| Full access to system Role and User Administration programs | 2 |
| Partial access to system Role and User Administration programs | 1 |
| Full access to product Role and User Administration programs | 2 |
| Partial access to product Role and User Administration programs | 19 |

El Paso County IT policy and data security best practices require the limited use of administrator accounts. The use of multiple accounts with elevated rights increases the overall risk to the system by allowing users to override internal controls. Furthermore, the elevated privileges granted by the administrator role pose a high risk to data and system security if any user credentials are compromised.

**Recommendation**

The Courts and Justice Software Management Team should review all administrative roles in the Enterprise Justice system. Special consideration should be given to the two roles with full access to system role and user administration programs. Ideally, only one role should have full access to system administration programs due to the previously outlined risks. Future role design should be reviewed and approved by the Enterprise Software Supervisor (Courts & Justice) or ITD management. User roles with administrative permissions designed for testing and troubleshooting should be limited to non-production environments to protect the integrity of the live data environment.

**Action Plan**

| Person Responsible | IT Division Manager - Software | Estimated Completion Date | February 2023 |
|---|---|---|---|

The IT department will review roles identified in the finding and update permissions as needed. Additionally, the department will work with data owners and the Courts and Justice Software User Group (CJSUG) for direction and approval of changes.

## FINDINGS AND ACTION PLANS

**Finding #2** **Risk Level** H

**User Assignment Design and Operation** – Multiple users both inside and outside ITD have been assigned roles with administrative rights. Users with these roles can override controls by modifying permissions granted to other users without proper authorization. User assignment analysis determined the following:

| User Assignment Determination | User Count |
|---|---|
| Full access to system Role and User Administration programs | 20 |
| Partial access to system Role and User Administration programs | 18 |
| Full access to product Role and User Administration programs | 38 |
| Partial access to product Role and User Administration programs | 465 |

El Paso County IT policy and the principle of least privilege requires that users be granted only the minimum necessary rights to perform their duties. These permissions should be in effect for the shortest duration necessary. Granting permissions to a user beyond what is necessary increases the risk of users obtaining or modifying system information in an unauthorized manner.

**Recommendation**

The Courts & Justice group should review all user permissions. Users outside of the core management team should not have access to modify roles. Users outside of the IT Help Desk and Software Management Team should not have permission to assign roles to others unless the outside user has been properly trained and all stakeholders understand the risks associated with the decentralization of user role assignment.

**Action Plan**

| Person Responsible | IT Division Manager - Software | Estimated Completion Date | April 2023 |
|---|---|---|---|

The IT department will review user assignments identified in the finding and update permissions as needed. Additionally, the department will work with data owners and the CJSUG for direction and approval of changes.

## FINDINGS AND ACTION PLANS

| Finding #3 | Risk Level (M) |
|---|---|

**Lack of Supporting Documentation** – The Courts & Justice group does not maintain adequate documentation for access control changes. Access control change logs were requested by the auditor, but it was determined that Enterprise Justice currently lacks the capability to maintain audit logs related to this function. As such, a review of this process is not possible at this time. Enterprise Justice HEAT ticket logs were requested but ITD determined providing specific reports from this application was not feasible at this time.

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 such change is not discovered upon management review.

**Recommendation**

The Courts & Justice group should maintain adequate access control change logs. These logs should be available to compare to available supporting documentation. The lack of this information greatly increases the risk that unauthorized permission changes are entered into Enterprise Justice and would not be discovered in a timely manner.

**Action Plan**

| Person Responsible | IT Division Manager - Software | Completion Date | July 2022 |
|---|---|---|---|

The IT department has created a manual access control change log sheet to capture updates, creation, or deletion of roles for the division. Additionally, the department will use the HappyFox service call management software to record and capture documentation required to make access control changes. The division Enterprise Software Supervisor (Courts & Justice) will regularly review the log and validate any changes.

| Finding #4 | Risk Level (M) |
|---|---|

**Stale Accounts** – The Courts & Justice group has adopted a 90-day user inactivation policy; however, a review of the current active users has identified 497 stale accounts out of a total of 2668 user accounts. Of the 497 stale accounts, 124 (25%) of these accounts have been inactive since their creation.

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

**Recommendation**

The Courts & Justice group should adhere to the 90-day user inactivation policy.

**Action Plan**

| Person Responsible | IT Division Manager - Software | Estimated Completion Date | July 2022 |
|---|---|---|---|

The department will work with data owners and the CJSUG to codify a policy to suspend/delete unused or orphaned accounts. Furthermore, the department will enforce the new policy and regularly monitor and disable stale accounts on a quarterly basis.

## FINDINGS AND ACTION PLANS

| Finding #5 | | | Risk Level (M) |
|---|---|---|---|
| **Management Change Review** – ITD management does not receive any change reports, nor do they have the ability to independently run reports related to Enterprise Justice access controls. The Enterprise Software Supervisor (Courts & Justice) currently monitors changes to the access control structure. However, the team supervisor also has the ability to maintain system access.<br><br>Best practices recommend monitoring whenever hard controls are not available. Inadequate review increases the risk that unapproved changes are implemented in the system or implemented access controls are overridden. | | | |
| **Recommendation** | | | |
| ITD management should begin to review changes or assign this oversight duty to an employee independent of the access control management function. This employee should have the ability to independently run change reports and review audit data. | | | |
| **Action Plan** | | | |
| **Person Responsible** | **IT Division Manager - Software** | **Estimated Completion Date** | **October 2022** |
| Management or responsible party will review control log and run reports related to access controls quarterly or as needed to review access control changes. | | | |

| Finding #6 | | | Risk Level (M) |
|---|---|---|---|
| **Policies and Procedures** – The Courts & Justice group currently operates on an unwritten set of policies and procedures. The team maintains informal, verbal agreements regarding access control management. These verbal agreements cover the software specialist, help desk, and IT trainer teams. The team supervisor expects to develop written policies and procedures with the assistance of the CISO and IT management team.<br><br>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 the Courts & Justice group will perform their duties in an inconsistent manner.<br><br>[1]COBIT is an IT management framework to help businesses develop, organize, and implement strategies around information management and governance. | | | |
| **Recommendation** | | | |
| The Courts & Justice group should document policies and procedures for the division. | | | |
| **Action Plan** | | | |
| **Person Responsible** | **IT Division Manager - Software** | **Estimated Completion Date** | **December 2022** |
| The department will update and document policies and procedures related to access controls. | | | |