Follow-up Review of Audit of Transit Division's Information Technology Operations

Office of the County Auditor

Follow-up Review Report

Robert Melton, CPA, CIA, CFE, CIG
County Auditor

Review Conducted by:
Kathie-Ann Ulett, CPA, Deputy County Auditor
Gerard Boucaud, CIA, CISA, CDPSE, Audit Manager
Luis Martinez, CISA, CDPSE, Information Technology Audit Supervisor

Report No. 23-08
February 22, 2023

OFFICE OF THE COUNTY AUDITOR
115 S. Andrews Avenue, Room 520 • Fort Lauderdale, Florida 33301 • 954-357-7590 • FAX 954-357-7592

February 22, 2023

Honorable Mayor and Board of County Commissioners

We have conducted a Follow-up Review of our Audit of Transit Division's Information Technology Operations (Report No. 20-01). The objective of our review was to determine the implementation status of our previous recommendations.

We conclude that of 30 recommendations in the report, 20 recommendations were implemented and 10 were partially implemented. We commend management for implementing our recommendations. The status of each of our recommendations is presented in this follow-up report.

Please be advised that the information presented herein is not considered an audit in accordance with Generally Accepted Governmental Auditing Standards. Had we conducted an audit, we may have identified additional findings and concerns.

We appreciate the cooperation and assistance provided by the staff of the Transit and Enterprise Technology Services Division throughout our review process.

Respectfully submitted,

Bob Melton
County Auditor

cc: Monica Cepero, County Administrator
Andrew Meyers, County Attorney
Kimm Campbell, Deputy County Administrator
Kevin Kelleher, Assistant County Administrator
Tim Garling, Deputy General Manager, Transportation Department

TABLE OF CONTENTS

IMPLEMENTATION STATUS SUMMARY

Implementation Status of Previous Recommendations From the
Audit of Transit Division's Information Technology Operations

REC. NO.	PREVIOUS RECOMMENDATION	IMPLEMENTED	PARTIALLY IMPLEMENTED	NOT IMPLEMENTED	NOT APPLICABLE
1.A	Ensure user access groups are adequately designed and documented to restrict activities based on job responsibilities and ensure that the following job functions are segregated: I. User Administration II. Application Development III. Business Transactions		☑		
1.B	Ensure appropriate procedures are in place to remove or disable terminated or transferred employee accounts within 24 hours of termination or transfer.		☑		
1.C	Ensure the use of generic accounts is restricted, where possible. In instances when these accounts must be used, management should ensure appropriate controls are in place to monitor user activity and tie that activity to authorized individuals.		☑		
1.D	Enhance application and system logging processes to: I. Ensure that logs are adequately secured, and access is appropriately limited.		☑		

REC. NO.	PREVIOUS RECOMMENDATION	IMPLEMENTED	PARTIALLY IMPLEMENTED	NOT IMPLEMENTED	NOT APPLICABLE
	II. Implement logs or appropriate monitoring activities in systems where logs are not currently available. Where required, management should work with application and system vendors to determine the feasibility of introducing functionality to effectively monitor high risk application changes such as user administrative activity or configuration changes. III. Ensure that logs either do not contain, or appropriately masks information that can be used to gain inappropriate access to applications and systems.				
2.A	Review, evaluate, and document the functional access granted to users by each role or user group on Transit's systems.		☑		
2.B	Ensure user access request forms contain sufficient information to demonstrate the level of access authorized by management.	☑			
3.A	Ensure all applications and systems meet or exceed the County's minimum password requirements. Any exceptions should be appropriately identified and mitigating controls which reduce the risk to an appropriate level documented.		☑		
3.B	Ensure available security features are appropriately designed and enabled.	☑			
4.A	Ensure physical access request forms are complete, appropriately authorized, and granted in accordance with the authorized requests.	☑			

REC. NO.	PREVIOUS RECOMMENDATION	IMPLEMENTED	PARTIALLY IMPLEMENTED	NOT IMPLEMENTED	NOT APPLICABLE
4.B	Prohibit Transit's Security section from issuing new physical access cards or modifying employee physical access rights unless they obtain the authorization to perform this function	☑			
5.A	Install mandatory updates in a timely manner.		☑		
5.B	Limit remote access to the Broward County Administrative Network to the authorized methods outlined in Volume 7: Chapter 3, section 15.3, of the County Administrative Policy and Procedure (CAPP).	☑			
6	Ensure financially and operationally significant applications have at least one dedicated secondary system environment where software releases can be tested prior to production implementation. In addition, environments in which applications are developed and tested should be segregated from production environments in which operational information processing is performed.	☑			
7	Enhance the user access review process to ensure it is complete and sufficiently detailed.		☑		
8.A	Handle incidents according to policy and procedures.	☑			
8.B	Enhance incident handling policies and procedures to appropriately categorize and handle all tickets in appropriate	☑			

REC. NO.	PREVIOUS RECOMMENDATION	IMPLEMENTED	PARTIALLY IMPLEMENTED	NOT IMPLEMENTED	NOT APPLICABLE
	timeframes established by management. These procedures should include how exceptions to established timeframes and incident processing are handled and approved.				
8.C	Require changes categorized and handled as emergency changes meet the appropriate criteria for emergencies.	☑			
9.A	Design and implement adequate monitoring controls to ensure data transferred between Fleetwatch and AssetWorks is complete.	☑			
9.B	Design and implement adequate monitoring controls to ensure management or system administrators are notified of data variances and transfer failures.	☑			
10.A	Immediately obtain sufficient licenses for the number of users on the Midas Systems and implement procedures to periodically monitor compliance with contract licensing provisions.	☑			
10.B	Ensure vendor performance objectives and incident response and resolution times are monitored against service standards in the vendor agreement.		☑		
11	Management test system restoration processes for mission critical IT Systems at least annually.	☑			
12.A	Evaluate the potential health risks associated with the current item storage practices in A and B above, and ensure policies and	☑			

REC. NO.	PREVIOUS RECOMMENDATION	IMPLEMENTED	PARTIALLY IMPLEMENTED	NOT IMPLEMENTED	NOT APPLICABLE
	procedures are appropriate to reduce the potential health risks to an appropriate level.				
12.B	Enhance physical security controls to ensure access to lost and found items is restricted to appropriate County personnel. I. If combination locks are used, management should implement procedures to periodically change the combination, and II. Management should ensure appropriate monitoring controls are in place, such as video surveillance, in order to detect inappropriate activity in a timely manner.	☑			
13.A	Work with the County Attorney to clarify the County's responsibility for handling lost and found items that may pose health and safety concerns to employees and members of the public, including illegal substances, and ensure procedures are updated accordingly.	☑			
13.B	Evaluate whether the retention of PII is required and, if so, ensure this information is adequately protected.	☑			
13.C	Ensure claimant information is consistently recorded and procedures governing lost and found property are followed.	☑			
13.D	Enhance inventory processes to ensure: I. Lost and found items are appropriately tagged and recorded in Returnity+.		☑		

REC. NO.	PREVIOUS RECOMMENDATION	IMPLEMENTED	PARTIALLY IMPLEMENTED	NOT IMPLEMENTED	NOT APPLICABLE
	II. Management performs and retains documentation of monthly inventory reconciliations.				
13.E	Ensure that: I. Items are destroyed or disposed of under dual control, and that adequate documentation is maintained II. Donation receipts are maintained for all items donated to third parties.	☑			
14	Enhancements to internal procedures and the continued exploration of technology to reduce the percentage of uncollected trip fares, including prepayment models for services provided.	☑			

INTRODUCTION

Scope and Methodology

The County Auditor's Office conducts audits of Broward County's entities, programs, activities, and contractors to provide the Board of County Commissioners, Broward County's residents, County management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We have conducted a follow-up review of our Audit of Transit Division's Information Technology Operations (Report No. 20-01). The objective of our review was to determine the implementation status of our previous recommendations.

Please be advised that the information presented herein is not considered an audit in accordance with Generally Accepted Governmental Auditing Standards. Had we conducted an audit, we may have identified additional findings and concerns.

Our follow-up review included such tests of records and other auditing procedures, as we considered necessary in the circumstances. The audit period was January 1, 2022, through December 31, 2022. However, transactions, processes, and situations reviewed were not limited by the audit period.

Overall Conclusion

We conclude that of 30 recommendations in the report, we determined that 20 recommendations were implemented and 10 were partially implemented. We commend management for implementing our recommendations. The status of each of our recommendations is presented in this follow-up report.

OPPORTUNITIES FOR IMPROVEMENT

This section reports actions taken by management on the Opportunities for Improvement in our previous review. The issues and recommendations herein are those of the original review, followed by the current status of the recommendations.

1. Access to County Data was not Restricted Based on Job Responsibilities, and Duties were not Adequately Segregated and Adequately Monitored

During our review of access to data and transactions within in-scope applications and their respective environments, we noted the following:

A. Management had not adequately designed user access groups to restrict access to Transit IT applications based on employee job responsibilities and segregation of duties restrictions as required by County Policy. Specifically, we noted that:

   I. For all seven systems reviewed, one or more users were inappropriately assigned access, granting them the ability to perform both administrator functions as well as business transactions creating a segregation of duties conflict.

   II. For five of the seven (71%) systems reviewed, management had not maintained appropriate security documentation and or institutional knowledge to determine whether the roles designed within applications were consistent with current user job responsibilities.

B. Account access for terminated and transferred employees was not consistently revoked from Transit applications, host servers and databases within 24 hours of employee termination. Specifically, we noted the following:

   I. Ten of 17 (59%) terminated employee accounts reviewed were not disabled or removed within 24 hours of employee termination. Two of the ten terminated employee accounts were still enabled at the time of our review. The remaining eight accounts were deactivated an average 45 days after the date of termination, with deactivations ranging from 9 to 130 days.

   II. Three of the seven (43%) systems reviewed contained enabled administrator accounts that belonged to employees who no longer worked for the County.

III. Five of seven (71%) systems reviewed contained enabled administrator accounts that belonged to employees who had transferred to different agencies in the County and no longer required access to Transit systems as part of their new job responsibilities.

C. Generic accounts were used to perform daily system and application administrative functions. Specifically, we noted:

I. Five of the seven (71%) application databases for in-scope applications were administered using shared, generic system accounts to perform database administration.

II. Five of the seven (71%) application and database servers supporting sampled applications had enabled, generic, administrator accounts that were not required for any existing business purpose.

D. We noted the following concerns with logging activities:

I. One of the seven (14%) applications reviewed allowed business users to delete application logs.

II. One of seven (14%) applications reviewed did not have the ability to produce security logs.

III. Two of the seven (28%) applications reviewed produced logs that contained information that could have been used to gain inappropriate access to applications and systems. Specifically, we noted:

a. One application log stored failed login usernames and passwords in plain text.

b. One application created a file on the user's workstations that logged the connection string information that contained the user's username and password in plain text.

We recommended management:

A. Ensure user access groups are adequately designed and documented to restrict activities based on job responsibilities and ensure that the following job functions are segregated:

I. User Administration

II. Application Development

III. Business Transactions

B. Ensure appropriate procedures are in place to remove or disable terminated or transferred employee accounts within 24 hours of termination or transfer.

C. Ensure the use of generic accounts is restricted, where possible. In instances when these accounts must be used, management should ensure appropriate controls are in place to monitor user activity and tie that activity to authorized individuals.

D. Enhance application and system logging processes to:

I. Ensure that logs are adequately secured, and access is appropriately limited.

II. Implement logs or appropriate monitoring activities in systems where logs are not currently available. Where required, management should work with application and system vendors to determine the feasibility of introducing functionality to effectively monitor high risk application changes such as user administrative activity or configuration changes.

III. Ensure that logs either do not contain, or appropriately masks information that can be used to gain inappropriate access to applications and systems.

Implementation Status:

A. Partially Implemented. For one of the in-scope applications, management designed documentation mapping employee job positions to functional access in the application. The design documents received the complete approval and signoff by both the subject matter experts and Transit management on February 6, 2023. Management stated that given the size of the BCT workforce, this project requires a significant commitment of time and resources. The Applications Team is in the process of reviewing all users across the in-scope applications and aligning roles with their job titles. Management indicated that they expect to complete the entire process by April 30, 2023.

We continue to recommend management work toward full implementation of our recommendations for all in-scope systems ensuring user access groups are adequately designed and documented to restrict activities based on job responsibilities and ensure that the following job functions are segregated:

I. User Administration

II. Application Development

III. Business Transactions

B. **Partially Implemented.** One of two application accounts reviewed was not disabled for 34 business days after the employee's termination. Additionally, two databases each included one active account granted elevated privileges assigned to terminated employees. The first, which had been identified during the previous review, had been terminated since February 13, 2015, and the second had been terminated since June 12, 2019. One of the two terminated employees accounts was secured during our review.

Management indicated that the other terminated employee account is no longer tied to a specifically named employee but is used as part of automated processes. Reprogramming the account name could create unnecessary risks to the functionality of one application.

We continue to recommend management ensure appropriate procedures are in place to remove or disable terminated or transferred employee accounts within 24 hours of termination or transfer.

C. **Partially Implemented.** We noted that all exceptions related to administrator accounts on the in-scope application and database servers have been addressed; however, of the database administrator accounts reviewed, three previously observed exceptions were not addressed. The generic administrative accounts previously noted as no longer required and scheduled to be removed from the database were not. Additionally, one of the three databases featured only default generic administrator accounts. Named accounts were created on this database to replace the generic accounts during our review.

Management indicated that they disabled two generic accounts in one application in the test environment and will remove the two accounts from the live production environment if there are no issues by February 20, 2023. The other generic administrator account is discussed above in relation to the employee's named account.

We continue to recommend management ensure that the use of generic accounts to administer systems are restricted where possible.

D. **Partially Implemented**.

I. **Implemented.**

II. **Partially Implemented.** One of the systems did not feature the inherent ability to generate security logs which restricts management's ability to review to

application configurations. Although management reached out to the vendor and received guidance regarding technical solutions which would allow transactions to be logged and monitored, they did not implement any of the potential solutions.

Management stated that this is a legacy system that is no longer supported by the vendor. Management is currently seeking to replace the application and it is expected that the new application will include adequate logging.

We continue to recommend management consider the implementation of monitoring controls over high-risk transactions. High risk application changes including user security, system or business code changes should be logged and monitored for appropriateness.

III. **Partially Implemented.** One of the two in-scope systems which produced files containing authentication information that could be used to gain inappropriate access to applications was modified to adequately remediate the issue. The second is no longer being supported by the vendor and as a result, management informed us that a technical solution is not feasible Management indicated that they have procured a replacement application that will be implemented in 18 to 24 months.

We continue to recommend management ensure that logs either do not contain, or appropriately mask information that can be used to gain inappropriate access to applications and systems. Additionally, where feasible, management should consider the implementation of compensating controls to reduce the risk that exposed user authentication information could be used to gain inappropriate access to the application.

2. User Administration Policies and Procedures Needed Enhancement

During our review of user administration policies and procedures for Transit's systems, we noted the following:

A. There was a lack of documentation describing the functional access granted to users by each role or user group on Transit's systems.

B. Access request forms submitted to Transit IT authorizing access to the in-scope applications were not consistently completed with adequate information to determine what level of access was authorized by management. We noted 14 of 20 (70%) user access request forms were approved without adequate information describing the required access.

We recommended management:

A. Review, evaluate, and document the functional access granted to users by each role or user group on Transit's systems.

B. Ensure user access request forms contain sufficient information to demonstrate the level of access authorized by management.

Implementation Status:

A. **Partially Implemented.** Management stated that a document with roles will be developed using new Applications Team personnel to better design roles for all applications, and subsequently create a Standard Operating Procedure based on that. As stated in response to paragraph 1A above, management approved the first set of user access design documents for one of the in-scope systems as of February 6, 2023. They stated that given the size of the BCT workforce, this project requires a significant commitment of time and resources. The Applications Team is in the process of reviewing all users and aligning roles with their job titles. Management indicated that they expect to complete the entire process by April 30, 2023.

   We continue to recommend management review, evaluate, and document the functional access granted to users by each role or user group on the remaining Transit's systems.

B. **Implemented.**

3. Password Requirements Needed Enhancement to Prevent Unauthorized Access and Ensure User Accountability

During our review of system password requirements, we noted following:

A. Six of the seven (86%) active systems reviewed did not meet the minimum password requirements set by County Policy.

B. Passwords and security features on one system used at Transit garages to control and monitor the dispensing of automobile fluids, including oil, transmission fluid, and diesel fuel had not been enabled or designed to reduce the risk of theft. We noted:

   i. A password or personal identification number (PIN) was not required.

   ii. The user identification information required to access the fluids was not restricted information and was commonly posted.

iii. Validation of vehicle information was disabled.

We recommended management:

A. Ensure all applications and systems meet or exceed the County's minimum password requirements. Any exceptions should be appropriately identified and mitigating controls which reduce the risk to an appropriate level documented.

B. Ensure available security features are appropriately designed and enabled.

Implementation Status:

A. **Partially Implemented.** Management partially addressed the recommendation by enabling single sign on and using Active Directory to manage user password security for two of the systems evaluated; however, two applications require updates to bring them into compliance with the County Administrative Policies and Procedures (CAPP). Additionally, three legacy applications do not feature settings which could be configured to enforce the CAPP requirements.

   Management has indicated that one legacy application was changed to meet CAPP requirements. The other two legacy applications do not feature settings that could be configured to meet CAPP requirements.

   We continue to recommend management ensure all applications and systems meet or exceed the County's minimum password requirements. Any exceptions should be appropriately identified and mitigating controls which reduce the risk to an appropriate level documented.

B. **Implemented**. Management configured security features to require valid vehicle information to be entered when enabling the pumps. Additionally, as of February 1, 2023, management has changed the security keys that were displayed in plain sight during our previous review.

4. Physical Access Requests were not Complete, Consistently Authorized, and Provisioned.

Management had a formal process for authorizing physical access within the agency; however, we noted the following:

A. Physical access was not consistently authorized and provisioned. We noted:

I. Thirty-six of the 42 (86%) physical access review forms reviewed were not appropriately authorized, lacking either the supervisor or the appropriate agency director signature required by Facilities Management Division, Security Office's Employee and Contractor ID Access Card Procedure.

II. Thirty-one of the 42 (74%) sampled employees were granted access inconsistent with the authorized physical access request form.

III. Physical access request forms did not consistently contain sufficient information to indicate the level of access approved by management

B. Transit's Security section issued new physical access cards (non-replacement) and modified physical access for Transit's employees without appropriate authority

We recommended management:

A. Ensure physical access request forms are complete, appropriately authorized, and granted in accordance with the authorized requests.

B. Prohibit Transit's Security section from issuing new physical access cards or modifying employee physical access rights unless they obtain the authorization to perform this function.

Implementation Status:

A. **Implemented**.

B. **Implemented**.

5. Only Approved Software Should have been Installed on County Servers, and Servers and Applications were not Patched in Accordance with County Policy.

During our review of Transit's IT System environments, we noted the following:

A. Four of the six (67%) applications hosted on servers residing on the Broward County Administrative Network were missing mandatory patches.

B. One of the six (17%) production application servers had unauthorized remote access tools installed and enabled.

We recommended management:

A. Install mandatory updates in a timely manner.

B. Limit remote access to the Broward County Administrative Network to the authorized methods outlined in Volume 7: Chapter 3, section 15.3, of the CAPP.

Implementation Status:

A. **Partially Implemented**. Sixteen vulnerabilities classified as "high" or "critical" severity were identified across 7 of the 9 in-scope servers. Ten of the vulnerabilities were addressed during our review; however, 6 had not been addressed, one of which was classified as "critical" severity.

   Management indicated that the vulnerability classified as critical severity relates to a legacy application. The legacy application is being replaced within 18 to 24 months. Management further indicated that it is aware of the remaining vulnerabilities and is in the process of remediating the remaining items. For one legacy application, management stated that they are in the process of designing mitigating controls to reduce the overall risk related to running the unpatched servers on the County's network including potential network segregation, activity logging and the monitoring of unusual activity on the respective servers.

   We continue to recommend management ensure mandatory updates are installed in a timely manner.

B. **Implemented.**

6. Application Control Environments were not Adequately Segregated

For three of the seven (43%) systems reviewed, development, quality assurance, and production environments were not adequately segregated. Specifically, we noted the following:

A. Two of the seven (29%) applications reviewed had only production environments. Vendor releases were deployed directly into production without testing.

B. One of the seven (14%) applications had its production and test environments on the same server.

We recommended management ensure financially and operationally significant applications have at least one dedicated secondary system environment where software releases can be

tested prior to production implementation. In addition, environments in which applications are developed and tested should be segregated from production environments in which operational information processing is performed.

Implementation Status: Implemented.

7. User Access Review Procedures Required Enhancement

Although management had implemented a formal process to perform periodic reviews of user access, we noted the following:

A. The review was not complete as follows:

   I. Accounts with access to dispense fluids at Transit garages were not included in the review. We noted two of 30 (7%) sampled employee accounts with the ability to dispense fluids no longer required access. Both accounts belonged to employees who had retired from the County.

   II. One of the seven (14%) applications was not included in the user access review process.

   III. Of the six user access reviews initiated for in-scope systems, one of the six (17%) received no response from management validating whether the active users had the appropriate access.

B. The review was not sufficiently detailed for one in-scope application. Two users had inadvertently been added to a legacy role that was granted unsegregated access to sensitive functions; however, this issue was not identified as part of the user access review.

We recommended management enhance the user access review process to ensure it is complete and sufficiently detailed.

Implementation Status: Partially Implemented. Management has updated policy and procedures and implemented a new process; however, user access reviews are not consistently completed for all accounts and in scope systems. Specifically:

A. Accounts for users who can dispense fluids were not included in the user access reviews provided

B. User access reviews were not performed for two of the in-scope systems during the audit period.

Management stated that a document with roles will be developed using new Applications Team personnel to better design roles for all applications, and subsequently create a Standard Operating Procedure based on that. As stated in response to paragraph 1A above, given the size of the BCT workforce, this project requires a significant commitment of time and resources. The Applications Team is in the process of will go back and reviewing all users and align roles with their job titles. Management indicated that they expect to complete the entire process by April 30, 2023. In addition, Management will save and file access review documentation for all accounts and in-scope systems. The SOP to enforce this will be completed in fiscal year 2023.

C. For four in-scope systems reviewed during the follow-up, we noted that 11 supervisors did not complete reviews of at least 1 user account, and we noted that 72 user accounts were not reviewed by the assigned supervisor / manager.

We continue to recommend management enhance the user access review process to ensure it is complete and sufficiently detailed.

8. Incident and Change Management Policies and Procedures Required Enhancement and were not Followed

Incident and change management policies and procedures were not consistently followed. During our review of incident and change management policies and procedures, we noted the following:

A. Of 3,988 incidents reviewed, 536 (13%) were not resolved within the timeframe defined in the ETS incident handling procedure. Additionally, of four distinct "priority 1" incidents that we observed during the audit period, two (50%) did not conform to documentation requirements outlined in the policy. One record was missing both the actions taken to resolve the issue and the root cause. The other incident was missing the root cause analysis. See items B and C below for additional issues affecting resolution time calculations and classifications.

B. A ticket system was used to track all work performed by IT support personnel including incidents; however, during our review, we noted:

   I. Not all tickets categorized as incidents met the definition of an incident outlined in the incident handling procedures.

   II. Incident handling procedures reviewed did not address how tickets that are not incidents should be handled.

III. Incident due dates were routinely changed without oversight or approval by management. There was no documented standard operating procedure governing this activity.

C. Change requests were inappropriately categorized as emergencies. Seven of the nine (78%) changes reviewed could not be reasonably justified as emergencies based on supporting documentation.

We recommended management:

A. Handle incidents according to policy and procedures.

B. Enhance incident handling policies and procedures to appropriately categorize and handle all tickets in appropriate timeframes established by management. These procedures should include how exceptions to established timeframes and incident processing are handled and approved.

C. Require changes categorized and handled as emergency changes meet the appropriate criteria for emergencies.

Implementation Status:

A. **Implemented**.

B. **Implemented**.

C. **Implemented**.

9. System Interfaces were not Adequately Monitored to Ensure Data Transfers are Complete

During our review of processes that moved data between applications, we noted the procedures used to determine whether data transferred between Fleetwatch and AssetWorks was complete required enhancement. Specifically, we noted management had not implemented:

A. A manual or automated process to match source and destination data totals after the data was transferred to ensure completeness.

B. Appropriate monitoring procedures to provide notification to management or system administrator in the event of failure.

We recommended management design and implement adequate monitoring controls to ensure:

A. Data transferred between Fleetwatch and AssetWorks is complete.

B. Management or system administrators are notified of data variances and transfer failures.

Implementation Status:

A. **Implemented**.

B. **Implemented**.

10. Contracts were not Routinely Monitored to Ensure Compliance

During our review to determine whether management monitored vendor performance against contract provisions, we noted:

A. Transit was out of compliance with contract licensing requirements for the Midas System. As of May 25, 2018, there were 751 active users and management had only procured 660 licenses. The estimated cost of obtaining these licenses using the 2017 fee schedule was a one-time licensing fee of $62,790 and $12,180 in annual maintenance.

B. Vendor performance objectives and incident response and resolution times were not monitored against the metrics outlined in the contracts.

We recommended management:

A. Immediately obtain sufficient licenses for the number of users on the Midas Systems and implement procedures to periodically monitor compliance with contract licensing provisions.

B. Ensure vendor performance objectives and incident response and resolution times are monitored against service standards in the vendor agreement.

Implementation Status:

A. **Implemented**.

B. **Partially Implemented**. Management has established formal standard operating procedures (SOPs) establishing periodic audits of the Information Technology Vendor Service Level Agreements (SLAs) to ensure compliance; however, management was

unable to demonstrate the reviews had been performed. Management stated that going forward, they plan to schedule audits, maintain documentation of their performance, and ensure the supporting documents are stored in a central repository consistent with the SOPs.

We continue to recommend management ensure vendor performance objectives and incident response and resolution times are monitored against service standards in the vendor agreement.

11. Continuity of Operations Plans (COOP) for Mission Critical IT Systems were not Tested Annually

While we noted Transit's COOP plan was adequate, system restoration processes for mission essential functions were not tested on an annual basis to determine whether systems could have been restored within stated recovery time objectives.

We recommended management test system restoration processes for mission critical IT Systems at least annually.

Implementation Status: Implemented.

12. Lost and Found Facilities and Storage Procedures were not Evaluated to Reduce Potential Health Risks and Increase Security.

Transit's lost and found item storage and work areas posed risks to the health and wellbeing of employees, and physical security controls needed to be enhanced. Specifically, we noted that:

A. The room where the Program Coordinator conducted day-to-day operations doubled as a storage room for damp molding clothes, prescription medication, and other potential hazardous items, such as syringes. Additionally, while conducting inventory testing, we identified used syringes where County employees needed to access inventoried items.

B. Some lost and found items were stored in a locked shipping container without temperature controls and ventilation. Although, we did not observe any potentially biohazardous items in the container during our site visit, a pungent odor emanated from the container when it was opened, requiring us to wait several minutes before entry.

C. Facilities security controls required enhancement. Specifically, we noted:

    I. Management used combination locks to secure storage containers; however, management had not implemented procedures to periodically change

combinations to ensure access is restricted to appropriate personnel. Management indicated that they were not aware of the last time the combination codes had been changed.

II. Monitoring controls such as video surveillance had not been implemented to monitor access and activity related to stored items. Management did not have any method of determining who accessed lost and found items or when.

We recommended management:

A. Evaluate the potential health risks associated with the current item storage practices in A and B above, and ensure policies and procedures are appropriate to reduce the potential health risks to an appropriate level.

B. Enhance physical security controls to ensure access to lost and found items is restricted to appropriate County personnel.

I. If combination locks are used, management should implement procedures to periodically change the combination, and

II. Management should ensure appropriate monitoring controls are in place, such as video surveillance, in order to detect inappropriate activity in a timely manner.

Implementation Status:

A. **Implemented**.

B. **Implemented**.

13. Lost and Found Operating Procedures Required Enhancement

During our review of the IT System used to manage lost and found inventory (Returnity+) and the standard operating procedures used to manage lost and found inventory, we noted the following concerns:

A. Lost and found procedures did not address special handling requirements for items such as:

- ❖ medicine,
- ❖ hazardous items, and
- ❖ illegal substances.

B. Personally Identifiable Information (PII) was not adequately protected. Through observation, we noted that copies of drivers' licenses and passports were stored in an unlocked desk in an administrative area of the Central Bus Terminal. Although the office could be secured by combination lock, we noted that the area was unlocked and accessible during our visit.

C. Procedures governing the final disposition of lost and found items were inconsistently followed:

   I. Five of 30 (17%) sampled items claimed did not have the required claimants photo identification recorded in Returnity+. One of the five did not have either the claimant's personal information or the form of identification reviewed on release of the item recorded.

   II. We noted one of 30 (3%) sampled items was released to a claimant by the Security Guard.

D. Inventory controls required enhancement, we noted:

   I. Lost and found items were not consistently tagged in accordance with Transit's Numbered Procedure Memorandum MTL-16, section 6.a.2. During our review, we noted two of the 10 (20%) lost items recorded in the database could not be located in inventory.

   II. Management did not maintain copies of monthly physical inventory performed and the reconciliation of results against the Returnity+ system. Management asserted that physical inventory reconciliations were performed; however, the documentation was not retained in order to demonstrate this activity

E. Procedures governing the donation and destruction of items outside of the 90-day retention guidelines were inconsistently followed. Specifically, we noted:

   I. Destruction logs were not consistently maintained to document the destruction or disposal of items.

   II. Donation receipts were not consistently maintained. Four of the 16 (25%) donations reviewed did not have a Broward County Transit Donation Receipt on file as required by Transit's procedures.

We recommended management:

A. Work with the County Attorney to clarify the County's responsibility for handling lost and found items that may pose health and safety concerns to employees and members of the public, including illegal substances, and ensure procedures are updated accordingly.

B. Evaluate whether the retention of PII is required and, if so, ensure this information is adequately protected.

C. Ensure claimant information is consistently recorded and procedures governing lost and found property are followed.

D. Enhance inventory processes to ensure:

   I. Lost and found items are appropriately tagged and recorded in Returnity+.

   II. Management performs and retains documentation of monthly inventory reconciliations.

E. Ensure that:

   I. Items are destroyed or disposed of under dual control, and that adequate documentation is maintained.

   II. Donation receipts are maintained for all items donated to third parties.

Implementation Status:

A. **Implemented**.

B. **Implemented**.

C. **Implemented**.

D. **Partially Implemented**.

   I. **Implemented.**

   II. **Partially Implemented**. While management retained documentation of the monthly review performed, we noted that the reviews did not include the complete inventory. Further we were informed that a complete inventory is not being performed. Monthly reviews capturing only items entered into inventory during a particular month are not adequate in ensuring that the physical inventory

matches the items on premises. Management agreed and stated that they plan to implement an annual inventory process and update their Lost and Found standard operating procedures accordingly. Management should ensure that a complete inventory is performed at least once, annually.

E. **Implemented**.

14. Paratransit Trip Fee Collection Procedures Required Enhancement

During our review of Adept application transaction processing, we noted that while transactions were processed as designed, drivers did not collect over $719,000 (40%) of the $1,815,128 in assessed trip fares between October 1, 2017, and September 30, 2018.

We recommended management consider enhancements to internal procedures and the continued exploration of technology to reduce the percentage of uncollected trip fares, including prepayment models for services provided.

Implementation Status: **Implemented.**