Audit of Transit Division's Information Technology Operations

Office of the County Auditor

Audit Report

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

Audit Conducted by:
Gerard Boucaud, CIA, CISA, Audit Manager
Luis Martinez, CISA, Information Technology Audit Supervisor
Muhammad Ramjohn, CISA, Information Technology Auditor

Report No. 20-01
October 3, 2019

Exhibit 1

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

October 3, 2019

Honorable Mayor and Board of County Commissioners:

We have conducted an audit of Information Technology Operations at the Transit Division. The objectives of our audit were to determine whether general and application information technology controls are adequate, and to determine whether any opportunities for improvement exist.

We conclude that general and application information technology controls are inadequate. Opportunities for improvement are included in the report.

We appreciate the cooperation and assistance provided by the Transit Division and Transportation Department throughout our review process.

Respectfully submitted,

Bob Melton
County Auditor

cc: Bertha Henry, County Administrator
Andrew Meyers, County Attorney
Monica Cepero, Deputy County Administrator
Chris Walton, Director of Transportation
Tim Garling, Deputy Director of Transportation

TABLE OF CONTENT

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 conducted an audit of Information Technology Operations at the Transit Division. Our audit objectives were to determine whether:

1. General and application information technology controls are adequate.

2. Any opportunities for improvement exist.

To determine whether general and application information technology controls are adequate, we selected a sample of systems, and reviewed information technology policies and procedures, and contract management processes. We assessed control environments, system and application user access permissions, system password requirements, system logs, and continuity of operations plans. We tested a sample of system changes, incident and change tickets, and data backup processes.

Our audit included an evaluation of the Transit Division's information technology (IT) general controls, which are controls that apply to all systems, components, processes, and data, such as; governance, security, change, data, operations, and incident management policies and procedures, that provide a stable operating environment and enhance the effective operation of specific business applications. In addition, we evaluated the implementation of these controls on the following business applications used by the Transit Division:

Business Application	Business Process
Adept	Paratransit
AssetWorks	Vehicle Inventory and Maintenance
Fleetwatch	Automotive Fluid Inventory and Dispensing
Genfare	Bus Fare Collections
Hastus	Bus Schedule Planning and Analysis

Business Application	Business Process
Midas	Bus Dispatching, Scheduling, and Staffing
Returnity +	Lost and Found

All other business applications used by the Transit Division were excluded from the scope of this audit.

We conducted this audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit included such tests of records and other auditing procedures, as we considered necessary in the circumstances. The audit period was January 1, 2017 through December 31, 2018. However, transactions, processes, and situations reviewed were not limited by the audit period.

Overall Conclusion

We conclude that general and application information technology controls are not adequate. Opportunities for improvement are included in the report.

Background

Mission & Operations

The Transit Division's (Transit) mission is to provide clean, safe, reliable, and efficient transit service to the community by being responsive to changing needs and focusing on customer service.

The public transportation system provides Broward County residents with access to a fleet of buses on fixed routes covering an area of over 410 square miles, including links to Miami-Dade and Palm Beach counties' transit systems, and Tri-Rail. In addition to fixed route services, Transit provides a complementary paratransit program, Transportation OPtionS (TOPS) to persons qualified under the Americans with Disabilities Act (ADA) of 1990 and Community Bus Service in partnership with 18 County municipalities.

Budget

For the 2018 Fiscal Year (FY), 1,083 positions were budgeted according to the adopted operating budget. The division's overall budget was an estimated $144.5 million. Table 1 shows actual amount for FY16 and FY17, and budgeted amounts for FY18

Table 1:Transit and Paratransit Transportation budget information for FY16 to FY18

	FY16 Actual	FY17 Actual	FY18 Budget	Positions FY18 Budget
Transit	$127,839,644	$135,052,990	$144,500,710	1083

Revenues consist of a combination of general funds, grants, taxes, and charges for services.

Information Systems

During the course of the audit, we reviewed a sample of the Information Technology (IT) systems managed primarily by Enterprise Technology Services (ETS) personnel embedded within the Transit Division. The IT systems reviewed include the following:

1. **Returnity+:** Transit utilizes Returnity + to manage lost and found items until the item is either returned to the rightful owner or an authorized recipient, donated or destroyed. This application is primarily used by the Customer Relations and Communications Section who oversee lost and found inquiries.

2. **Fleetwatch:** Transit utilizes Fleetwatch to manage the dispensing and inventory of automotive fluids such as oil, transmission fluids and diesel fuel. This application is primarily used by Transit's maintenance section for the fueling and servicing of busses.

3. **Assetworks:** Transit utilizes Assetworks to manage every aspect of a vehicle fleet, including comprehensive preventive maintenance schedules, work orders and labor tracking, as well as parts and inventory management. This application is also used by Transit's maintenance section to support maintenance operations.

4. **ADEPT:** Transit utilizes ADEPT for reservations, scheduling, dispatch, customer service, and management of Paratransit services. This application is used by the Paratransit Section, which administers a shared-ride service for persons with physical, cognitive, emotional, visual, or other disabilities which functionally prevent them from using the County's fixed-route bus system permanently, temporarily or under certain conditions. The program is subject to federal and state mandates such as the ADA and Chapter 427, Florida Statutes.

5. **Hastus:** Transit utilizes Hastus to plan, analyze, and schedule bus operations. This application is used by the Transportation Operations Section for managerial, operational, and administrative support to ensure that bus service is provided throughout the transit system.

6. **Midas:** Transit utilizes Midas for dispatching and scheduling to ensure staffing levels are adequate to support operations, to ensure regulations are adhered to, and to monitor route performance on a day-to-day basis. This application is also used by the Transportation Operations Section.

7. **Genfare:** Transit utilizes Genfare to manage bus fares, record fare payment, and collect ridership data. This application is also used by the Transportation Operations Section.

Incident Management

ETS has documented policies and procedures in place covering incident management procedures. These procedures include incident definitions, priority levels based on incident severity, and steps covering how the different priority levels should be handled and in what timeframe.

Change Management

ETS has documented policies and procedures covering change controls processes. Changes to IT system environments are made up of ordinary changes and emergency changes. Ordinary changes include scheduled modifications to existing applications such as enhancements, patches, or minor bug fixes. These procedures include controls that ensure changes to application environments on the County's network are scheduled and managed to reduce risk. Procedures include:

- Documenting the change request
- A formal assessment
- Planning
- Designing and Testing
- Implementation and Review
- User Acceptance

Emergency changes bypass the standard change process because, inherently, they require immediate resolution.

OPPORTUNITIES FOR IMPROVEMENT

Our audit disclosed certain policies, procedures and practices that could be improved. Our audit was neither designed nor intended to be a detailed study of every relevant system, procedure, or transaction. Accordingly, the Opportunities for Improvement presented in this report may not be all-inclusive of areas where improvement may be needed.

1. Access to County Data Should be Restricted Based on Job Responsibilities, and Duties Should be 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 has 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. Administrator functions include the ability to change how an application functions and to change user capabilities, either at an individual user or user group level. This access is incompatible with the ability to perform business transactions as it allows users the ability to bypass automated controls increasing the risk of inappropriate or unauthorized activity.

II. For five of the seven (71%) systems reviewed, management has not maintained appropriate security documentation and or institutional knowledge to determine whether the roles designed within applications are consistent with current user job responsibilities. Without this information, management has no assurance that the access approved and granted to employees remains commensurate with employee job responsibilities increasing the risk of unauthorized or inappropriate activity and improper segregation of duties.

IT System	Was Adequate Security Documentation Maintained?	Was There Compensating Institutional Knowledge for System that Lacked Adequate Documentation?
Adept	Yes	Yes
AssetWorks	No	No
Fleetwatch	No	No
Genfare	No	No
Hastus	No	No
Midas	No	No
Returnity +	Yes	Yes

Broward County IT Administration Policy, Volume 7: ETS Chapter 3, Section 5.2l, requires employees to be given only the access required to perform job responsibilities (least privilege). Limiting access to systems plays a critical role in decreasing the risk of inappropriate or unauthorized activity. Granting excessive access increases the opportunities for unauthorized modification and misuse of information.

B. Account access for terminated and transferred employees is 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 belong 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.

Broward County IT Administration Policy, Volume 7: ETS Chapter 3, Section 4.2 a and d, states access rights must be revoked immediately upon termination notification and that agency management must ensure that all access rights have been removed accordingly. Failure to disable or remove user accounts for employees who are terminated or

transferred increases the risk of unauthorized access and inappropriate activity on County systems.

C. Generic accounts are used to perform daily system and application administrative functions. A generic or shared role account is an account designed for a specific role that can be used by more than one person (e.g. administrator, system). 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.

   The use of generic user accounts to administer applications and servers reduces user accountability as activity performed by these accounts cannot be tied to a single individual. As a result, they increase the risk of unauthorized system changes and limit management's ability to take disciplinary action when erroneous or inappropriate activities are detected using these accounts.

D. We noted the following concerns with logging activities:

   I. One of the seven (14%) applications reviewed allows business users to delete application logs. County Administrative Policy and Procedures (CAPP), Volume 7 ETS, Chapter 3, section 7.4.c, require that logs be protected from unauthorized modification, access, or destruction. Without securing system logs, management cannot ensure system activity and events are effectively and reliably monitored.

   II. One of seven (14%) applications reviewed does not have the ability to produce security logs which restricts management's ability to review changes to application configuration. High risk application changes including user security, system or business code changes should be logged and monitored for appropriateness.

   III. Two of the seven (28%) applications reviewed produce logs that contain information that can be 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 making it easy to guess the actual username and passwords. Utilizing these

logs, we were able to guess three user account passwords and gain access to the system in a controlled test with Transit IT.

b. One application created a file on the user's workstations that logs the connection string information that contains the user's username and password in plain text. Although this file is purged when the application session terminates, this information can be used to gain inappropriate or unauthorized access.

We recommend 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.

Management's Response:

A. Management Agrees: BCT's Information Technology (BCT IT) Section and BCT management will design and document a Standard Operating Procedure to restrict activities based on job responsibilities and ensure job functions are properly segregated. BCT will be performing a comprehensive review of all system user roles. This review will lay out the road map to update the various user responsibilities associated with the applications. BCT anticipates this review will be completed by the end of March 2020.

B. Management Agrees and has Implemented: The Transportation Department implemented a new procedure on September 30, 2019 to ensure all employees who have separated from the Transportation Department have their accounts removed or disabled within 24 hours.

C. Management Agrees: BCT IT will immediately begin working with application vendors to remove generic system accounts for the cited applications, to the extent it is technically possible. BCT IT will complete this activity by the end of October 2019. For the cited application and database servers with generic accounts that were not required for any existing business purpose, the generic accounts were removed as of September 30, 2019.

D. Management Agrees: BCT IT will immediately begin working with application vendors to eliminate the exposure of inappropriate access described in Opportunity for Improvement 1, Section D, Part Ill. BCT IT will work with applicable vendors to determine the feasibility to improve application log monitoring and security, to the extent it is technically possible. BCT IT anticipates completing the assessment and resulting remediation activities by the end of February 2020.

2. User Administration Policies and Procedures Need Enhancement

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

A. There is a lack of documentation describing the functional access granted to users by each role or user group on Transit's systems. Many of these roles or groups were designed many years ago for a variety of purposes; however, adequate documentation was not maintained to describe their purpose. User access roles should be documented and mapped to clearly define and appropriately segregate business processes. Without documentation, management may not have a clear understanding of the access they are authorizing for each user and does not have assurance that user access is restricted based

on employee job responsibilities and adequate segregation duties as required by County policy.

B. Access request forms submitted to Transit IT authorizing access to the in-scope applications are 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. User access request forms should contain sufficient information to demonstrate the level of access authorized by management. Without adequate documentation, additional inquiries must be performed by IT personnel in order to grant access, increasing the risk that the access granted is inappropriate, and no record is maintained of the access authorized by management.

We recommend 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.

Management's Response:

A. Management Agrees: BCT will design a Standard Operating Procedure to document the functional access granted to users by each role or user group on Transit's systems. BCT anticipates completing this activity by the end of March 2020.

B. Management Agrees: The BCT IT Section will design and document a Standard Operating Procedure to ensure that user access request forms contain sufficient information to demonstrate the level of access authorized by management. Completing this activity is dependent on information gathered in the response above. BCT anticipates completing this activity by the end of March 2020.

3. Password Requirements Should be Enhanced 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. ETS Administration, CAPP, Volume 7, Chapter 2, Section 6.1 set password requirements for user accounts. Additionally, to ensure

compliance with the standard password policies, Volume 7, Chapter 3, section 5.2.K, indicates that application logins must use Active Directory authentication whenever possible.

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 have not been enabled or designed to reduce the risk of theft. We noted:

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

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

   iii. Validation of vehicle information is disabled.

   This combination of security weaknesses listed above allows any employee with access to the garage to dispense fuel without accountability and limits management's ability to determine whether fluids dispensed were used for an appropriate business purpose, increasing the risk of theft.

Authentication to systems provides a method to confirming the identity of the user. Authentication methods, such as passwords represent the digital keys to County systems and should be configured to meet or exceed the minimum-security standards established by the County to reduce the risk of inappropriate activity.

We recommend 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.

Management's Response:

A. Management Agrees: The BCT IT Section will evaluate all password requirements for the cited applications in accordance with CAPP, Volume 7: Chapter 2. BCT IT will work with all vendors to implement mitigations for password requirements. BCT IT anticipates completing this activity by the end of February 2020. All future software procurements will require vendors to meet mandatory password requirements.

B. Management Agrees: The BCT's Maintenance Section will design and document a Standard Operating Procedure to establish a fuel dispensing process which will include the enabling of security features in the fuel dispensing system. The procedure will ensure user identification information to access fluids is restricted and will require valid vehicle information upon the dispensing of fluids. BCT anticipates completing this activity by the end of October 2019.

4. Physical Access Requests Should be Complete, Consistently Authorized, and Provisioned.

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

A. Physical access is 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 resulting in instances where the identical access requested for employees resulted in different access rights granted to Transit's facilities.

Facilities Management Employee and Contractor ID / Access Card Procedures require supervisor and agency director signatures as valid authorization and that all relevant information must be completed including authorized signatures, access required, and day and time needed. Failure to adequately complete and authorize physical access requests increases the risk of unauthorized or inappropriate access to County facilities.

B. Transit's Security section issues new physical access cards (non-replacement) and modifies physical access for Transit's employees without appropriate authority resulting in noncompliance with County policy and increasing the risk of inappropriate physical access. We noted Transit's Security section was granted a policy exception allowing them to issue replacement cards only. The policy exception states that all other actions are to

be performed by Facilities Management including all new and modified access to Transit's facilities.

We recommend 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.

Management's Response:

A. Management Agrees: The BCT Safety, Security and Compliance Section is developing a new Standard Operating Procedure and will ensure access forms received are complete and contain all the information needed for processing, and that the level of authorization granted is appropriate for the individual's position. All BCT physical access authorizations will require the approval of the Transportation Department Director or designee. BCT anticipates completing this activity by the end of October 2019.

B. Management Agrees and has Implemented: Effective July 1, 2019, BCT's Safety, Security and Compliance Section no longer issues new or replacement ID cards. BCT does and will continue to modify and/or change door access requests only for the Transit facilities at Copans and Ravenswood garages, Broward Central Terminal, Northeast Transit Center and the West Terminal, in accordance with the Facilities Management Division (FMD) Employee and Contractor ID/Access Card Procedures.

   Notwithstanding and to ensure compliance with Facilities Management's procedures, BCT is developing new internal Transit Standard Operating Procedures for:

   - Initially approving requests for replacement ID cards, obtaining the approval of the Department Director or designee, and then submitting the request to FMDSecurity for final approval and processing;

   - Initially approving requests for door access to non-Transit County facilities (i.e. Government Center East and West, etc.), obtaining the approval of the Department Director or designee, and then submitting the request to FMD Security for final approval and processing; and,

- Modifying and/or changing door access requests to Transit facilities at Copans and Ravenswood garages, Broward Central Terminal, Northeast Transit Center and the West Terminal and obtaining the approval of the Department Director or designee in accordance with the Facilities Management Division (FMD) Employee and Contractor ID/Access Card Procedures.

BCT anticipates completing this activity by the end of October 2019.

5. Only Approved Software Should be Installed on County Servers, and Servers and Applications Should be 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, which are a set of changes designed to update, fix, or improve a system. ETS IT Administrative CAPP, Volume 7: Chapter 3, Sections 2 & 3, outline policies and procedures governing patch management, and indicate that all servers, both physical and virtual must follow the ETS Patch Management procedure. These procedures include ETS Security and Compliance verifying patch installations through network and host vulnerability scanning. Unpatched systems on the Broward County Administrative Network increase the risk that known vulnerabilities can be exploited.

B. One of the six (17%) production application servers had unauthorized remote access tools installed and enabled. Broward County IT Administration Policy, Volume 7: Chapter 3, Section 15.3 outlines approved methods for accessing the Broward County Administrative Network (BCAN) remotely. Servers utilizing unsupported or unapproved remote access tools increases security and operational risks to the Broward County Administrative Network.

We recommend 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.

Management's Response:

A. Management Agrees and has Implemented: The BCT IT Section developed and implemented a reboot schedule to ensure that patches are applied in a timely manner. This was completed on August 1, 2019.

B. Management Partially Agrees: The vendor for the production application server cited is limited to the specific remote access tool to provide maintenance and support services to BCT. Currently, the BCT IT Section has mitigating controls for the cited application to limit remote access to the vendor. Access is only activated and granted when BCT IT resources are physically available to monitor the vendor's activity in real-time and access is immediately terminated by BCT IT upon completion of these activities.

6. Application Control Environments Should be 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 have only production environments. Vendor releases are deployed directly into production without testing, increasing the risk to system stability, data and processing integrity, and security.

B. One of the seven (14%) applications has its production and test environments on the same server, increasing the risk that testing issues could negatively impact production performance, or cause system outages to occur.

System environments should be adequately segregated to support change processes such as development, quality assurance, pre-production and production as required.

We recommend 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.

Management's Response: Management Agrees: One of the applications was remediated by creating a testing environment in March of 2019. The other application includes a complex operating environment and infrastructure. BCT IT determined that it would not be cost beneficial to duplicate the entire system in a test environment (including various fluid dispensing equipment); however, the BCT IT Section will implement a testing environment for software

upgrades and database upgrades. BCT IT anticipates completing this activity by the end of March 2020.

The application with production and testing on the same server is a legacy application which has licensing and physical key constraints which prevent the BCT IT Section from separating the production and testing environments. BCT is planning to upgrade this application by December 2020. The upgraded software will not require a physical key and will enable BCT IT to establish separate hosting environments for test and production.

7. User Access Review Procedures Require Enhancement

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

A. The review is not complete as follows:

   I. Accounts with access to dispense fluids at Transit garages are not included in the review to ensure their continued appropriateness. 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 may not be 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.

ETS IT Administrative CAPP, Volume 7, Chapter 3, Section 4 contains provisions requiring agencies and data owners to periodically review user access rights for accuracy. Failure to adequately conduct user access reviews may allow employees to retain inappropriate access after a change in job function, termination from Broward County or after an organizational change has occurred.

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

Management's Response: Management Agrees: The BCT IT Section will design and document a Standard Operating Procedure to ensure the BCT IT section performs a yearly review of user access to all Transit applications, eliminates discrepancies and ensures management responds, and approves, all user access reviews requested. BCT IT anticipates completing this activity by the end of March 2020.

8. Incident and Change Management Policies and Procedures Should be Enhanced and Followed

Incident and change management policies and procedures are 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 is 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 meet the definition of an incident outlined in the incident handling procedures.

   II. Current incident handling procedures reviewed do not address how tickets that are not incidents should be handled. Such tickets include requests for new or enhanced features, or services.

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

   Incidents should be appropriately categorized and handled consistently according to documented policies and procedures. Without adequate incident handling procedures, management is not able to determine whether incidents are handled appropriately in the timeframes required by management to maintain operational performance, and management may not able to rely on performance metrics when making decisions.

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. Emergency changes bypass the standard change process because inherently emergency changes require immediate resolution. System changes should not be handled as emergencies unless justified as these types of changes present a higher a risk of error to system operations.

We recommend 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.

Management's Response:

A. Management Partially Agrees: The current resolution of incidents has an on-time performance of 87% which is above the industry standard benchmark of 82% for on-time incident resolution. This benchmark is set by Pink Elephant, an international consulting and training company that measures IT management metrics and collects, analyzes and presents IT management metrics benchmarks. BCT IT agrees to continue to follow ETS policies and procedures for incident handling.

B. Management Agrees and has Implemented: The County's ETS Division has implemented a new ticketing system to address these findings. The new ticketing system accommodates requests for new or enhanced features and categorizes incidents appropriately. The system went live on August 19, 2019.

C. Management Agrees and has Implemented: The BCT IT Section has established a process to review and document, via the ticket management system, that a valid emergency change is required. The BCT IT Section has established governance to ensure there is adequate documentation to support emergency changes. This change was implemented June of 2019.

9. System Interfaces Should be Adequately Monitored to Ensure Data Transfers are Complete

During our review of processes that move data between applications, we noted the procedures used to determine whether data transferred between Fleetwatch and Assetworks is complete require enhancement. Specifically, we noted management has not implemented:

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

B. Appropriate monitoring procedures to provide notification to management or system administrator in the event of failure; for example, if the data file was not generated

Adequate monitoring controls for system interfaces ensure data and process integrity. Failure to adequately monitor data transfer activity increases the risk that data and processing errors remain undetected.

We recommend 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.

Management's Response:

A. Management Agrees: The BCT IT section will establish an automated process to match source and destination data. BCT IT anticipates completing this activity by the end of March 2020.

B. Management Agrees: The BCT IT section will establish an automated process to notify support personnel in the event of failure. BCT IT anticipates completing this activity by the end of March 2020.

10. Contracts Should be Routinely Monitored to Ensure Compliance

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

A. Transit is 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. Contract licensing requirements should be periodically monitored to ensure compliance. Failure to comply with contract requirements, including user licensing increases the County's legal risk. Management took immediate steps to remediate this issue once notified.

B. Vendor performance objectives and incident response and resolution times are not monitored against the metrics outlined in the contracts. Vendor performance against contract requirements should be monitored and periodically evaluated. Without monitoring vendor performance against contract requirements, management may not be aware of whether they are receiving the level of service paid for.

We recommend 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.

Management's Response:

A. Management Agrees: A Work Authorization was executed with the vendor in June of 2019 to bring licensing up-to-date. Additionally, the BCT IT Section will design and document a Standard Operating Procedure to monitor licensing requirements with vendors. BCT IT anticipates completing this activity by the end of March 2020.

B. Management Agrees: The BCT IT Section will design and document a Standard Operating Procedure to monitor, measure and enforce Services Level Agreements with vendors. BCT IT anticipates completing this activity by the end of March 2020.

11. Continuity of Operations Plans (COOP) for Mission Critical IT Systems Should be Tested Annually

While we noted Transit's COOP plan is adequate, system restoration processes for mission essential functions are not tested on an annual basis to determine whether systems can be restored within stated recovery time objectives. System restoration processes ensure systems and data can be restored from established backups to facilitate recovery from a disaster. These procedures should be regularly tested to ensure they remain adequate as systems and infrastructure evolves. Without periodically testing system restoration procedures, management

cannot be reasonably assured that they will be able to restore services in accordance with the recovery objectives established in their COOP after a disaster.

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

Management's Response: Management Agrees: BCT will work with ETS to engage a 3rd party vendor to perform a business impact analysis to identify Transit's critical applications and develop a test and restoration plan. BCT is expected to complete this activity in collaboration with ETS by March 2020.

12. Lost and Found Facilities and Storage Procedures Should be Evaluated to Reduce Potential Health Risks and Increase Security.

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

A. The room where the Program Coordinator conducts day-to-day operations doubles 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 need to access inventoried items.

B. Some lost and found items are 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. The storage containers house a mix of items in a heated non-ventilated environment.

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

    I. Management uses combination locks to secure storage containers; however, management has 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 have not been implemented to monitor access and activity related to stored items. Management does not have any method of determining who accessed lost and found items or when.

Storage practices should maintain the integrity of the lost and found process as well as ensure the wellbeing of employees and the public. Improper storage practices and inadequate physical security increase health risks to County employees and the public, as well as reputation risks to the County should lost and found items be stolen.

We recommend 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.

Management's Response:

A. Management Agrees and has Implemented: The Lost and Found Customer Service Representative will dispose of all soiled and odorous items immediately by placing them in a disposal bin to be picked up with daily trash collection. BCTs remedy for prescription medication will be to document and store found medications in a locked container for five business days, then drop off unclaimed medications at a nearby pharmacy under the FDA's Safe Drop Program which allows for the disposal of unused, unwanted and expired medications at no cost to BCT. This process was implemented on August 15, 2019.

    Any syringes found or turned into Lost and Found will be safely handled with the use of protective gloves and will be placed in biohazard containers which will be taken to the Florida Department of Health for disposal weekly. This process was implemented on August 23, 2019.

    In addition, effective July 1, 2019, the Lost and Found Agent has been instructed to open the current container and only enter when conditions are favorable.

B. Management Partially Agrees and has Implemented: Effective July 1, 2019, all lock combinations were changed. In the future, the combinations will be changed

immediately upon a change in personnel assigned to Lost and Found. In addition, BCT will ensure that only approved Customer Service staff are allowed in the area.

BCT does currently have a video monitoring system in place which views the Lost and Found Storage Room. These video monitors are checked throughout the day by Customer Service Supervisors at the Broward Terminal and at the main BCT Offices at Government Center West.

13. Lost and Found Operating Procedures Should be Enhanced

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 do not address special handling requirements for items such as:

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

These items should be securely stored under conditions that maintain public safety and the viability of any returnable items. If these items are inappropriately stored, they may pose a health risk to County employees as well as members of the public who may claim these items.

B. Personally Identifiable Information (PII) is not adequately protected. Through observation, we noted that copies of drivers' licenses and passports are stored in an unlocked desk in an administrative area of the Central Bus Terminal. Although the office is secured by combination lock, we noted that the area was unlocked and accessible during our visit. PII should be adequately secured and restricted to authorized personnel. Failure to adequately secure PII increases the County's legal risk.

C. Procedures governing the final disposition of lost and found items are 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. Transit's policies and procedures require that claimant's

information be maintained. Without adequate claimant's information, management may unable to demonstrate the disposition of the item or resolve disputes.

II. We noted one of 30 (3%) sampled items was released to a claimant by the Security Guard. Transit's procedures establish that the Marketing Manager is assigned responsibility over the receipt, control, and disposition of lost and found items, and Customer Service Center (CSC) staff representatives assigned to the Broward Terminal are responsible for the safeguarding, processing, handling, and disposition of these items. Management should ensure that only authorized personnel release items to claimants. Failure to ensure only authorized personnel release items increases the risk of inappropriate activity.

D. Inventory controls require enhancement, we noted:

I. Lost and found items are 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. Item tags facilitate the accurate tracking and locating of items. Lack of asset tags increases management's difficulty in locating and reconciling lost and found items.

II. Management does not maintain copies of monthly physical inventory performed and the reconciliation of results against the Returnity+ system. Management asserts that physical inventory reconciliations were performed; however, the documentation was not retained in order to demonstrate this activity. Monthly physical inventory reconciliations provide management with timely notification of errors and inappropriate activity. Management should retain documentation of this activity in order to demonstrate its due diligence and to ensure all items are accounted for properly. Failure to maintain this documentation increases the risk that items can be lost, misplaced, or stolen without detection.

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

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

II. Donation receipts are 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.

Destruction logs and donation receipts document the disposition of lost and found items if they remain unclaimed. Without adequate documentation of item disposition, items may be lost or stolen without detection.

Lost and found policies and procedures should be complete and cover all significant areas of operations. Failure to have comprehensive policies and procedures increase the risk of lost, misplaced, and misappropriated items; increases health and safety risks to employees and the public; and reduces management's ability to enforce consistent operations and compliance with laws and regulations related to lost and found items and protected information.

We recommend 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.

Management's Response:

A. Management Agrees and has Implemented: BCT reviewed its Lost and Found responsibilities with the County Attorney's Office and the following procedures have been developed.

   As discussed above, BCT's remedy for prescription medication is to document and store found medications in a locked container for five business days then drop off unclaimed medications at a nearby pharmacy under the FDA's Safe Drop Program which allows for the disposal of unused, unwanted, and expired medications at no cost to BCT. This process was implemented on August 15, 2019.

   Any hazardous items found or tuned in to Lost and Found, such as syringes, will be safely handled with the use of protective gloves and will be placed in biohazard containers which will be taken to the Florida Department of Health for disposal as needed. This process was implemented on August 23, 2019.

   Effective July 1, 2019, any illegal substances turned into Lost and Found are immediately turned over to the Fort Lauderdale Police Department/Broward County Sheriff's Office.

B. Management Agrees and has Implemented: Effective July 1, 2019, BCT implemented a process where staff will no longer retain personally identifiable information but will visually verify the claimant's identification. Once identification is established, claimant will be required to sign the Property Case Report Form to receive lost property. The Lost and Found Customer Service Representative will also sign the form to verify the lost items were returned. Documentation will be disposed of in accordance with Broward County's record retention policy.

C. Management Agrees and has Implemented: Effective July 1, 2019, BCT implemented a process where staff will no longer retain personally identifiable information but will visually verify the claimant's identification. BCT will ensure that the Property Case Report form is completed properly and signed by claimant and Customer Service Lost and Found Representative before property is returned. Additionally, BCT's policy has always been that Lost and Found Customer Service staff or designees are the only personnel authorized to release items to claimants. Customer Service and Security staff have been re-trained on these procedures and the Customer Service Supervisor will monitor for compliance.

D. Management Response: Customer Service staff will conduct an audit of the Returnity+ system to identify items recorded in the database but not found in the inventory. Items

not found in the inventory will be removed from the Returnity+ system. The audit is anticipated to be concluded by December 31, 2019. Regarding monthly inventory reconciliations by Management, monthly physical inventory reconciliations have been conducted by Customer Service Management on an ongoing basis. Effective August 15, 2019, Customer Service implemented a process where the documentation of these reconciliations is reviewed, verified, reported to senior management and retained.

E. Management Agrees and has Implemented: Effective August 15, 2019, a process to document all items donated to third parties has been implemented. This Customer Service process will ensure that items are destroyed or disposed of under dual control in accordance with the governing procedures, and that adequate documentation is maintained.

14. Paratransit Trip Fee Collection Procedures Should be Enhanced

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. The paratransit TOPS Rider's Guide states fares are required upon entering the vehicle and failure to pay may result in loss of transportation privileges. Depending on the applicant's approval qualifications, their one-way required fare amount could range between $0 and $3.50. Management informed us neither Transit, nor the contracted service providers perform collections functions and will provide the service to customers even if the customers do not pay. In addition, we noted no procedures exist to prevent clients who do not pay consistently from scheduling trips.

We conducted a survey soliciting responses of neighboring municipalities to compare their Paratransit fee collection processes against Broward County Paratransit's and noted the following:

County	Is Payment Required When Boarding the Paratransit Vehicle?	Is a prepayment system in place (i.e., prepaid voucher / ticket)?	Are patrons typically allowed to continue to book rides if they have not paid for past trips?	Collection actions taken (if any) to collect unpaid fees.	Approximate % of collected trip fees from total trip fees charged for fiscal year.
Broward	Yes	No	Yes	None	60%
Miami Dade	Yes	Yes	Yes	None, clients may face suspension of service for repeated incidents.	99%

County	Is Payment Required When Boarding the Paratransit Vehicle?	Is a prepayment system in place (i.e., prepaid voucher / ticket)?	Are patrons typically allowed to continue to book rides if they have not paid for past trips?	Collection actions taken (if any) to collect unpaid fees.	Approximate % of collected trip fees from total trip fees charged for fiscal year.
Palm Beach	Yes	Yes	Yes	None.	99%
Hillsborough (Sunshine)	No	No, customers are billed via invoice at months end.	Yes, until 90 days past due.	Past due invoices, sent to customers, phone calls, then suspension.	85%
Hillsborough (Hart)	Yes	Yes	No fare / No ride.	N/A	N/A
Lake	Yes	No	Yes	No Response	No Response
Jacksonville (City)	Yes	Yes	Yes	No Response	No Response
Pinellas	Yes	Yes	Yes, but must pay balance owed upon next trip boarding.	Collected upon arrival at destination, upon return home, or upon pick-up for next trip.	100%

Information was compiled by the Office of County Auditor based on survey responses, and municipality website information. No additional procedures were performed to validate the accuracy of the responses received or the data published on municipality websites.

During our review, we noted under the United States Department of Transportation Code of Federal Regulations Title 49, Section 37.125(h), an entity may establish an administrative process to suspend, for a reasonable period of time, the provision of complementary paratransit service to ADA eligible individuals who establish a pattern or practice of missing scheduled trips. Additionally, we reached out to the Federal Transit Administration (FTA) for their opinion with regards to fare evasion and collection processes. They stated to ensure nondiscrimination, a good practice is for an agency to have written rules of rider conduct and related internal policies. They specified these policies would apply equally to complementary and fixed route services, as well as to riders with and without disabilities. Further, they informed us that there is no requirement to provide complementary paratransit service for riders who don't pay the fare, just as a transit agency might not allow a fixed route user with or without a disability to board fixed route vehicle without paying.

We recognize this service is mandated by Federal Law, it serves a vulnerable population, and the cost of providing this service greatly exceeds the revenue generated. Because of the vulnerable population that is served by this system, it is important to have collection and enforcement policies that take into account the need for transportation by those who have little or no funds available for payment.

We recommend 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.

Management's Response: BCT will review these policy change recommendations with Broward County Administration to determine what, if any, policy changes will be recommended for implementation. Please note that it has been the policy of Broward County to ensure that the County's Transportation Options (TOPS) customers, the community's most vulnerable population, have access to transportations services for essential and life-sustaining trips. The nature of this transit service lends to prioritizing the provision of service over denying a critical trip due to the nonpayment of fare. In addition, BCT constantly evaluates industry best practices and the introduction of new technologies that enhance the convenience of using and paying for TOPS service. BCT received approval in January 2019 from the Broward County Commission to evaluate the feasibility of using the Rider's Choice Pilot payment card to provide an alternative to customers from paying cash for their fare. In addition, BCT is evaluating other prepayment methods and will make recommendations on future fare collection technology.