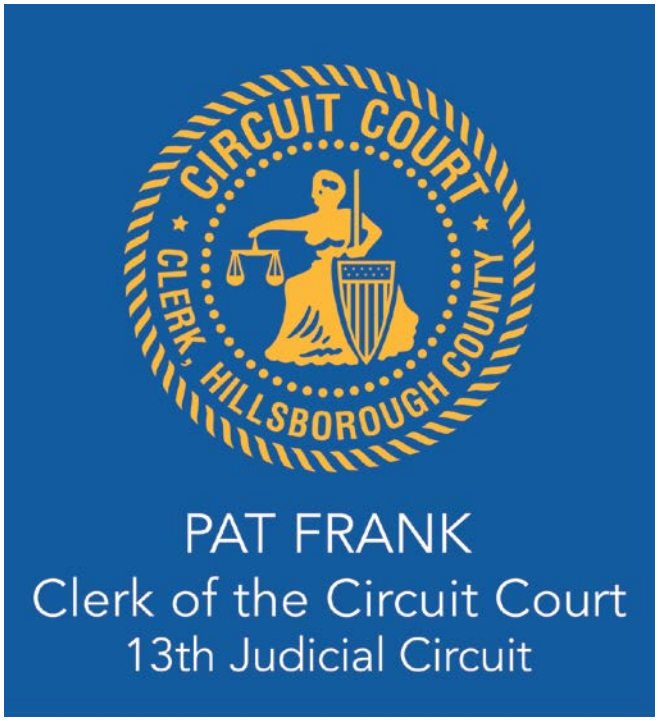

COUNTY AUDIT

HILLSBOROUGH COUNTY, FLORIDA

PUBLIC UTILITIES DEPARTMENT
ACCOUNT INFORMATION MANAGEMENT SYSTEM (AIMS)

REPORT # 242

DECEMBER 27, 2012

December 27, 2012

The Honorable Ken Hagan, Chairman
The Honorable Kevin Beckner
The Honorable Victor D. Crist
The Honorable Al Higginbotham
The Honorable Lesley "Les" Miller, Jr.
The Honorable Sandra L. Murman
The Honorable Mark Sharpe

Dear Chairman Hagan and Commissioners:

County Audit performed an audit of the Public Utilities Department Account Information Management System (AIMS), Audit Report #242, dated December 27, 2012. Responses to our recommendations were received from the Director of Public Utilities and are included in the report after each audit comment and recommendation.

County Audit appreciates the cooperation and professional courtesies extended to the Audit Team by the Director and personnel of the Public Utilities Department during this audit.

Sincerely,

Peggy Caskey, CIA, CISA, CFE
Director, County Audit

cc: Mike Merrill, County Administrator
Lucia Garsys, Deputy County Administrator
John Lyons, Department Director
Bruce Dangremond, Manager, Performance Mgmt, Business and Support Services

TABLE OF CONTENTS

THIS PAGE LEFT BLANK INTENTIONALLY

EXECUTIVE SUMMARY

BACKGROUND INFORMATION:

The Account Information and Management System (AIMS) is used by the Public Utilities Department for managing customer accounts. The AIMS performs key functions such as billing, deposits, and refunds. Customers can: make payments by visiting a cashier in a Public Utilities office; initiate payments through PC Banking; send payments by mail; make payments on the telephone through the Interactive Voice Response (IVR) system; and make payments on the Internet through the Interactive Web Response (IWR) system. Refunds are processed then electronically transmitted to FAMIS where the Accounts Payable Division of County Finance completes the refund and issues a check to the customer.

Security within the AIMS is accomplished with roles based on the employee's job description. A limited number of personnel within the Public Utilities Department have the ability to change configuration settings and update user security. Changes to the functionality of the AIMS go through a formal change management process. A user must submit a System Management and Technical Issue Resolution Register (SMATIRR) ticket to request a change. The change is tested in a separate development environment and approved by management before it is implemented in production.

OBJECTIVE:

Assess the Public Utilities Department's segregation of duties, appropriateness of assigned roles, changes to customer accounts, and the refund process within the AIMS.

SCOPE:

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* issued by The Institute of Internal Auditors. The audit period was from August 1, 2010, through September 30, 2012.

OVERALL EVALUATION:

The Public Utilities Department was responsive to our inquiries and provided thorough information when requested. We found knowledgeable and dedicated employees that were receptive to our suggestions for improvements. Our audit identified several opportunities to strengthen and improve controls related to the AIMS.

The following table summarizes the Audit Comments contained within this report. For each Audit Comment, a cross-reference to the page number where the details of the Audit Comment can be found has been included.

AUDIT COMMENT	DESCRIPTION	PAGE REFERENCE
1	Opportunities exist to enhance the employee account change process.	See page 3 of this report.
2	Opportunities exist to enhance the procedure for customer refunds.	See page 5 of this report.
3	Opportunities exist to enhance the configuration change management process.	See page 7 of this report.
4	System security for passwords needs to be improved.	See page 9 of this report.
5	AIMS user access management controls need improvement.	See page 11 of this report.

OPINION:

Based on the results of our audit testing, the controls over the AIMS need improvement. We believe that our recommendations, if implemented, will enhance the internal controls used to carry out the assigned responsibilities of the Public Utilities Department.

The exit conference was conducted on November 1, 2012.

AUDIT BY:

Mark Kolman, Audit Manager, CPA, CIA, CISA, CFE
Heidi Pinner, Senior Auditor, CIA, CFE, CRMA
Marc Hogan, Auditor II

AUDIT COMMENTS & RECOMMENDATIONS

Control Activities: Listed below are Audit Comments that represent opportunities for the Public Utilities Department to strengthen the internal controls used to carry out the Department's responsibilities. For each Audit Comment, a recommendation has been included.

AUDIT COMMENT 1

Opportunities exist to enhance the employee account change process.

Due to a lack of monitoring controls, employees could make changes to their own customer accounts which may go undetected. On February 1, 2012, management drafted Policy PUD-3.001; *Accessing a Public Utilities Department Employee Account(s)*which requires employees to declare associated accounts and prohibits them from making changes to these accounts. To date, this Policy has not been implemented. Employee customer accounts have not been identified in the AIMS therefore, management is unable to review changes to these accounts to ensure no unauthorized changes have been made.

RECOMMENDATION:

To provide adequate monitoring of employee account changes, consideration should be given to the following:

1. Formally implement Policy PUD-3.001; *Accessing a Public Utilities Department Employee Account(s).*

2. Incorporate flags or identifiers for employee associated customer accounts in the AIMS.

3. Incorporate automated notifications to trigger a management level review of all employee account changes.

CLIENT RESPONSE:

1. ***Concur***

2. ***Concur***

3. ***Concur***

CORRECTIVE ACTION PLAN:

1. *Policy No. PUD-3.001 (Accessing a Public Utilities Department Employee Account(s) was approved October 2, 2012 and will be implemented.*

2. *Employee associated customer accounts in AIMS will be flagged with an "Employee Account" alert for those staff with AIMS change capability.*

3. *Automated monthly reports will be developed for management level review of "Employee Account" flagged accounts.*

TARGET COMPLETION DATE:

1. February 1, 2013

2. March 1, 2013

3. March 1, 2013

AUDIT COMMENT 2

Opportunities exist to enhance the procedure for customer refunds.

Controls in place to verify refund eligibility prior to disbursement are not included in the documented Accounts Payable System Generated Refund procedure. The current procedure indicates that a verification of refund eligibility is performed by accounting staff but does not indicate the process or criteria used for this verification.

Business process procedures are intended to formalize a process to ensure consistency, identify training opportunities, and manage performance. All procedures should include current information and reflect any changes or updates to the business process. The Accounts Payable System Generated Refund procedure should include all required steps and applicable criteria to verify and process a customer account refund.

RECOMMENDATION:

To ensure procedures for customer refunds are adequately documented, communicated, understood and adhered to, consideration should be given to the following:

1. Update the Accounts Payable System Refund Procedure to incorporate the process and criteria used to verify refund eligibility. This could be accomplished within the current procedure or by reference to a separate process detail, checklist, etc.

2. Ensure that all applicable staff members are adequately trained on the procedure.

3. Monitor for compliance with the procedure.

CLIENT RESPONSE:

1. ***Concur***

2. ***Concur***

3. ***Concur***

CORRECTIVE ACTION PLAN:

1. *The "AIMS Refund Report Procedures" document outlining process and criteria used to verify refund eligibility was added to the Accounting Team's business processes on November 9, 2012.*

2. *All Public Utilities Department staff members responsible for Accounts Payable refund reviews will be adequately trained on "AIMS Refund Report Procedures"*

3. *Compliance will be monitored monthly by reviewing reports in directory: \WRS-BSOC\ GROUPS\AIMS FINANCIALS\AIMS FINANCIALS FY(yy)\REFUNDS\REFUNDS(mmyyyy) and documented by email approval notification to the Clerk of the Circuit Court's staff.*

TARGET COMPLETION DATE:

1. November 9, 2012

2. February 1, 2013

3. February 1, 2013

AUDIT COMMENT 3

Opportunities exist to enhance the configuration change process.

AIMS configuration changes are not adequately documented in the System Management and Technical Issue Resolution Register (SMATIRR). Configuration changes occur when a system user requests a change to how the system functions or performs. A simple example of a configuration change would be a conversion of a five digit zip code field to allow for a nine digit zip code. Configuration changes have the potential to significantly affect a system's performance and the total effect of a configuration change often cannot be gauged until put into use. For these reasons, a configuration change process should be in place to adequately control and document the lifecycle of the change. Adequately documenting and monitoring this process also helps to ensure consistency, continuity and accountability.

The System Management and Technical Issue Resolution Register is set up as a queue system to route change requests through the configuration change process but does not capture a holistic record of the issues' lifecycle and various approvals.

Per management, a manual review of sign-off forms is conducted at weekly System Administration and System Support meetings but this review is not documented.

RECOMMENDATION:

To ensure AIMS configuration changes are adequately documented, consideration should be given to the following.

1. Establish a process to capture a record of the complete configuration change process and approvals.

2. Document the review and approval of sign-off forms for configuration changes at the weekly System Administration and System Support meetings.

CLIENT RESPONSE:

1. Concur

2. Concur

CORRECTIVE ACTION PLAN:

1. The "AIMS Configuration Changes" business process was updated October 31, 2012, to include documentation of configuration change process and approvals for milestones in Development, Testing and Production environments.

2. The AIMS Systems Analyst and Principle Business Analyst will update the configuration change documents with their electronic signatures or automated log entry indicating their

review and approval during the System Administration and System Support meetings, when a configuration change is required; followed by a monthly review by the AIMS System Administration Section Manager.

TARGET COMPLETION DATE:

1. October 31, 2012

2. March 1, 2013

AUDIT COMMENT 4

System security for passwords needs to be improved.

The current configuration of the AIMS limits the Public Utilities Department's ability to comply with the Hillsborough County Information & Technology Services (ITS) Information Security Standard**:** 11.3.1- Password Use. This standard includes the following requirements:

11.3.1.2 *All System - level passwords (e.g., root, NT admin, application admin accounts, etc.) should be changed on at least a quarterly basis, except where the application or device has limitations which preclude the password being changed that frequently. The frequency with which those passwords are changed should take into account the risk involved should the password be compromised.*

11.3.1.12 *Temporary or "first use" passwords should be changed the first time that the authorized user accesses the system.*

New AIMS users are provided with a system generated default password. The AIMS does not prompt the user to create a new password for his account and does not allow the user to change his password. The AIMS maintains a record of each user password and the Security/CIS Admin group has access to this password list.

Static passwords and maintenance of a retrievable password list poses a significant risk to system security by increasing the opportunity for unauthorized access.

RECOMMENDATION:

To ensure compliance with the ITS Information Security Standard 11.3.1- Password Use, consideration should be given to the following.

1. Continue to work with the AIMS vendor to inquire about password change functionality in future releases of the software.

2. Continue to research possible single sign-on access for regular users of the software.

3. To mitigate the potential for passwords to be inappropriately accessed or disclosed, examine and monitor the methods used to generate and distribute passwords.

CLIENT RESPONSE:

1. Concur

2. Concur

3. Concur

CORRECTIVE ACTION PLAN:

1. *A service request will be submitted to the AIMS vendor to include password change functionality in future application releases.*

2. *Staff will research the possibility to utilize single sign-on access for AIMS regular users.*

3. *The "AIMS System Security" business process will be reviewed to determine if additional opportunities exist to mitigate inappropriate access or disclosure of user passwords.*

TARGET COMPLETION DATE:

1. February 1, 2013

2. March 1, 2013

3. March 1, 2013

AUDIT COMMENT 5

AIMS user access management controls need improvement.

The Public Utilities Department is not in compliance with the Hillsborough County Information & Technology Services (ITS) Information Security Standard 11.2 - User Access Management. This standard includes the following requirements:

11.2.1.5 The user's immediate manager and/or supervisor should periodically reevaluate the system privileges granted to a user to determine whether currently enabled system privileges are still needed to perform the user's current job duties.

11.2.4.3 Management and security administration should conduct periodic checks on privileges granted each user to ensure that unauthorized access has not been obtained.

- Per management, the System Security group meets with team leaders annually to evaluate individual user access and user group privileges. Written procedures are not in place to formalize this review and supporting documentation does not indicate when the review was conducted, who made the decision for user access changes or how changes were verified upon completion.

11.2.1.3 Users should sign (physically or electronically) a confidentiality agreement and an information system security agreement indicating that the user understands the conditions of access prior to being given a user ID that allows access to County systems.

- Per management, system users are not required to sign confidentiality/security forms acknowledging their responsibilities as AIMS users. A training course is available for new users of the software but it does not require users to sign or certify understanding of the conditions for system access.

11.2.1.9 Management should promptly report all significant changes in end-user duties or employment status to the appropriate security administrator handling the user IDs of the affected persons.

- Per management, a review of user groups and user access is conducted annually. A separate process is not in place to ensure that changes in employment status or duties will be addressed immediately.

11.2.2.1 Users should be allocated privileges with the minimum access required for their job function on a need-to-use basis.

- During our review we noted that the billing user group had inappropriate access granted. Users in this group were granted a privilege which should have been exclusive to the billing manager.

11.2.2.3 All user ID creation, deletion and privilege change activity performed by systems administrators and others with privileged user IDs should be logged and periodically reviewed.

- Per management, these reviews are conducted quarterly but no written procedure is in place to review activity of system administrators or other privileged users. User activity logs are maintained for these individuals but do not include any verification of review or sign off.

ITS Information Security Standard 11.2 is designed to provide assurance that users have the appropriate system access and that they understand the conditions and responsibilities related to that access. Non-compliance with this Policy limits that assurance.

RECOMMENDATION:

To ensure Department user access controls are in place, functioning and in compliance with the ITS Information Security Standard 11.2, consideration should be given to the following:

1. Develop a formal procedure for the review of user access privileges. Supporting documentation for this review would ideally include evidence of the timing of the review, responsible decision makers and a post review verification of updates made to user access.

2. Require users to sign confidentiality/system security agreements prior to granting access to the AIMS.

3. Develop a mechanism to ensure that changes in employment status or duties triggers a review of the user's access rights

4. Correct the access rights of the billing user group.

5. Develop a formal procedure to document the logging and review of system administrators or privileged user activity and maintain evidence of this review.

CLIENT RESPONSE:

1. Concur

2. Concur

3. Concur

4. Concur

5. Concur

CORRECTIVE ACTION PLAN:

1. A written procedure for review of user access privileges will be added to AIMS security business processes; documentation of reviews will include team lead(s) and the AIMS security staff sign-off with dates memorializing the review and update process.

2. The "Acknowledgement of Professional Responsibility Concerning Access To and Disclosure of Hillsborough County Customer Information" form was developed and implemented 10/29/2012 for all new AIMS users; forms will be obtained from existing users.

3. The AIMS System Administration will review options available to identify and report AIMS users that have changed status or their position number through data obtained from HRIS.

4. "Billing Manager" user right "delete bill segment" was removed from the "Billing" user group on October 11, 2012.

5. Written procedure "AIMS Admin and Super User Auditing" was added to business process on October 31, 2012.

TARGET COMPLETION DATE:

1. February 1, 2013

2. February 1, 2013

3. March 1, 2013

4. October 11, 2012

5. October 31, 2012

THIS PAGE LEFT BLANK INTENTIONALLY