TO: The Honorable Chairman and Members of the Board of County Commissioners

FROM: Ken Burke
Clerk of the Circuit Court
Ex Officio County Auditor

SUBJECT: Follow-Up Audit of ACF2 Mainframe Security Software

DATE: December 22, 2010

For your review and filing in the Official Records, I am enclosing a copy of the follow-up audit dated December 22, 2010 on the above-referenced audit.

I hope you find this report helpful in ensuring Pinellas County government provides the best possible service to our citizens.

cc: Robert S. LaSala, County Administrator
Jim Bennett, County Attorney
Paul F. Alexander III, Executive Director, Business Technology Services
Claretha N. Harris, Chief Deputy Director, Finance Division
Ernst & Young
FOLLOW–UP AUDIT OF ACF2 MAINFRAME SECURITY SOFTWARE

Audit Services
Division of Inspector General

Ken Burke, CPA*
Clerk of the Circuit Court
Ex Officio County Auditor

Hector Collazo, Jr., CFE, CFS, CISA, CIG, CIGI
Inspector General/Chief Audit Executive
Division of Inspector General**

Audit Team
Melissa Dondero, CPA*, CIA, CIGA – Inspector General Auditor II
Scott Stees, CIGA, CIGI, CIA, CFE, CISA, CGFO – Senior Inspector General Auditor

DECEMBER 22, 2010
REPORT NO. 2010-19

*Regulated by the State of Florida
**Accredited Office of Inspector General
By the Commission for Florida Law Enforcement Accreditation
December 22, 2010

The Honorable Chairman and Members
of the Board of County Commissioners

We have conducted a Follow-Up Audit of the ACF2 Mainframe Security Software. The objective of our review was to determine the implementation status of our previous recommendations.

Of the five recommendations contained in the audit report, we determined that two have been implemented and three have been partially implemented. The status of each recommendation is presented in this follow-up review.

We appreciate the cooperation shown by the staff of Business Technology Services during the course of this review.

Respectfully Submitted,

Hector Collazo, Jr., Director
Audit Services, Division of Inspector General

Approved:

Ken Burke, CPA*
Clerk of the Circuit Court
Ex Officio County Auditor

*Regulated by the State of Florida
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Introduction</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status of Our Recommendations</strong></td>
<td></td>
</tr>
<tr>
<td>1. Appropriate Access Controls Are Not In Place For Datasets Containing Sensitive Fiscal Information.</td>
<td>6</td>
</tr>
<tr>
<td>2. ACF2 Global System Options Are Not Set To Enforce County Password Policies.</td>
<td>8</td>
</tr>
<tr>
<td>3. No Systematic Process Exists For Review Of ACF2 Logging And Violation Reports.</td>
<td>12</td>
</tr>
<tr>
<td>4. Changes To The ACF2 Configuration Are Not Properly Reviewed And Authorized.</td>
<td>13</td>
</tr>
<tr>
<td>5. No Formal Written Policies And Procedures Have Been Established For Maintaining ACF2 Software.</td>
<td>15</td>
</tr>
</tbody>
</table>
INTRODUCTION

Scope and Methodology

We conducted a follow-up audit of the ACF2 Mainframe Security Software. The purpose of our follow-up audit is to determine the status of previous recommendations for improvement.

The purpose of the original audit was to:

1) Determine if ACF2 software secures the integrity, accuracy, privacy and confidentiality of the data and resources on the Mainframe system.
2) Determine if ACF2 reporting of security incidents is adequate.
3) Determine if administration of ACF2 software is adequate.

To determine the current status of our previous recommendations, we conducted an interview with management to determine the actual actions taken to implement recommendations for improvement. We performed limited testing to verify the process of the recommendations for improvement.

Our follow-up audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing and Standards for Offices of Inspector General, and, accordingly, included such tests of records and other auditing procedures, as we considered necessary in the circumstances. Our follow-up testing was performed during the months of November and December 2010. The original audit period was May 1, 2007 through May 1, 2008. However, transactions and processes reviewed were not limited by the audit period.

Overall Conclusion

Of the five recommendations in the report, we determined that two have been implemented and three have been partially implemented. However, the following risks are still present:

A. The review of the ACF2 security structure is informal and does not take place on a scheduled basis resulting in the risk that not all areas are rotated through periodically and important datasets may not be adequately protected.

B. Three former County employees continue to have access to ACF2. These individuals have read, write, allocate and execute access to any dataset beginning with "FIS" although write and allocate access is logged. These Financial datasets are not adequately protected.
C. Several Pinellas County Information Security Policy requirements are not met with the current Global System Option settings resulting in the risk that passwords chosen by Mainframe users may not be strong and could easily be compromised. Weak passwords leave critical data and resources vulnerable to unauthorized access.

D. The manual review of ACF2 logging and violation reports is inefficient and there is a risk that problems may be overlooked since specific thresholds for violation investigations and escalation procedures to process the report still have not been drafted.

We commend management for the implementation of two of our recommendations and continue to encourage management to fully implement the remaining three recommendations.

Background

The Pinellas County Business Technology Service Department (BTS) has utilized ACF2 software to provide security over its mainframe system since 1986. ACF2 (more formally, CA-ACF2; Computer Associates-Access Control Facility) is a product from Computer Associates that enables security on mainframes. The County’s mainframe contains several applications such as finance applications, the Criminal Justice Information System applications and official records.

ACF2 prevents accidental or deliberate modification, corruption, mutilation, deletion, or viral infection of files. ACF2 enables an organization to strengthen security, streamline administration, and provide enhanced auditing capabilities, including managing user identities and access to assets, monitoring of accesses and reports, enforcement of business policies, compliance with regulations and achievement of end-to-end security management. With ACF2, no action is required to secure data. All data is protected until the owner of the data or another authorized individual grants access. This approach reduces the likelihood of exposure through omission of security controls.

Since initial installation of ACF2, many changes have occurred in the Pinellas County’s computing environment that would necessitate review and modification of ACF2 settings. Throughout our review, staff responsible for ACF2 administration has been adjusting the configuration of the software to meet the security needs of the County.

The County has adopted Information Technology Infrastructure Library (ITIL) methodology to deliver a framework of best practice approaches that can help align BTS with business requirements, improve service quality, and lower the long-term cost of IT service provisions. Originally developed by the British government in the late 1980s, today ITIL is the world’s most widely accepted approach to IT Service Management.

The administration of ACF2 software requires services to support installing, configuring, changing, and upgrading the software. The concept of Service Support for Change Management and Release Management are approaches under the ITIL methodology.
STATUS OF RECOMMENDATIONS

This section reports our follow-up on actions taken by management on the Recommendations for Improvement in our original audit of ACF2 Mainframe Security Software. The recommendations contained herein are those of the original audit, followed by the current status of the recommendations.

1. Appropriate Access Controls Are Not In Place For Datasets Containing Sensitive Fiscal Information.

Current ACF2 rules do not adequately protect financial accounting data. We sampled financial accounting datasets to evaluate if appropriate access controls are in place to protect sensitive fiscal information. Financial accounting datasets include files of the Clerk of the Circuit Court's financial system that include General Ledger, Payroll, Accounts Payable and Accounts Receivable. We also reviewed other accounting and collection systems datasets including Fee Accounting, Traffic, Civil/Small Claims, Juvenile, Tax Collector, Property Appraiser, Sheriff and other in-house IT programs. We identified every user who has access to the sampled datasets and users who have the authority to change the dataset rules, even though roles and responsibilities should never allow them to have access to these systems or datasets. We found that several programmers have access to the accounting and collection systems production datasets; however, alterations were logged, and access has since been removed for these individuals.

Appropriate segregation of duties requires that programmers be separated from production since the two functions are inherently incompatible. Since programmers have detailed knowledge of the applications' logic and access to the computers operating system and utilities, a programmer could make unauthorized or unintentional changes to the application. The programmer is also able to conceal fraudulent programming among legitimate programming. To ensure the correctness and integrity of the financial systems, an appropriate control is for all modifications to the datasets be made in a test environment and a separate group, usually a quality assurance group moves the updates into production. The County may not have the staff to support this optimal division of duties. A mitigating control is to limit the access to a select few and have their access logged.

Since none of the modifications made by programmers to financial accounting datasets are logged, there is no audit trail or timely independent review. Unauthorized or erroneous programming could be introduced undetected, affecting the County's financial transactions. Although there are valid reasons for a select few to have access to financial accounting datasets, documentation must be produced and maintained to support modifications. Audit trails can provide a means to help accomplish several security related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem analysis. An audit trail should include sufficient information to establish what events occurred and who (or what) caused them. In general, an audit trail should specify when the event occurred, the

Audit Services, Division of Inspector General
Clerk of the Circuit Court
Page 6
user ID associated with the event, the program or command used to initiate the event, and the result. Limiting access and logging will help achieve appropriate security.

According to COBIT 4.0, DS5 Ensure Systems Security:

"The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimize the business impact of security vulnerabilities and incidents."

Further, DS5.3 Identity Management states:

"All users (internal, external and temporary) and their activity on IT systems (business application, system operation, development and maintenance) should be uniquely identifiable. User access rights to systems and data should be in line with defined and documented business needs and job requirements. User access rights are requested by user management, approved by system owner and implemented by the security-responsible person. User identities and access rights are maintained in a central repository. Cost-effective technical and procedural measures are deployed and kept current to establish user identification, implement authentication and enforce access rights."

There has been a general lack of review of access rights to sensitive fiscal information on the Mainframe. The ACF2 security group grants access to datasets based on the system’s owner requests. The system owners may not have a security scheme developed to understand how to properly grant access to their system. Inadequately protected datasets allow users to modify essential system data intentionally or unintentionally. This poses significant risk to the reliability of the data in the financial systems.

Recommendation:

Management limit full access to the financial accounting datasets to a core group of staff responsible for maintaining the data, and this access be logged in ACF2. We also recommend management perform a periodic review of the security structure. This review should be initiated by IT, directing system owners to review security roles, responsibilities and access rights. All areas should be rotated through periodically to ensure important datasets are adequately protected.

Status:

Partially implemented. Management limited full access to the financial accounting datasets to a core group of staff responsible for maintaining the data, and this access is logged in ACF2. However, three individuals (MISTS00, MISTS21 and CLKDP11/CLKDP21) have access to
ACF2 that are no longer employed by the County. These individuals have read, write, allocate and execute access to any dataset beginning with "FIS" although write and allocate access is logged. The periodic review of the security structure is informal and does not take place on a scheduled basis. Having a more formal, regularly scheduled review process will ensure all areas are rotated through periodically to ensure important datasets are adequately protected.

Management Response:

The logon IDs identified above have unique access authority that needs to be preserved. Each of these IDs have been reassigned to current County employees to ensure that the production environment can continue to be effectively managed and maintained.

2. ACF2 Global System Options Are Not Set To Enforce County Password Policies.

Several Global System Options (GSO) for password controls are not consistent with the Pinellas County Information Security Policy and other applicable policies, standards and generally accepted security principles. GSO records define ACF2 system-wide options and include various operating parameters and user-defined exits that are important for security over the system. Our review of the active GSO for password controls found the following deficiencies, summarized in the table and discussed below.

<table>
<thead>
<tr>
<th>POLICY</th>
<th>Global System Options PASSWORD Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Difficult-to-Guess</td>
<td></td>
</tr>
<tr>
<td>Alphabetic character required</td>
<td>No alphabetic character required</td>
</tr>
<tr>
<td>User’s logon ID as password prohibited</td>
<td>User’s logon ID as password allowed</td>
</tr>
<tr>
<td>Numeric character required</td>
<td>No numeric character required</td>
</tr>
<tr>
<td>Alpha-numeric passwords required</td>
<td>All numeric passwords allowed</td>
</tr>
<tr>
<td>Character required</td>
<td>National or user-defined character not required</td>
</tr>
<tr>
<td>Reserved word prefixes prohibited</td>
<td>Reserved word prefixes allowed</td>
</tr>
<tr>
<td>B. Cyclical Passwords Prohibited</td>
<td></td>
</tr>
<tr>
<td>Similarity checking performed</td>
<td>Similarity checking not performed</td>
</tr>
<tr>
<td>Reserved word prefixes prohibited</td>
<td>Reserved word prefixes allowed</td>
</tr>
<tr>
<td>C. Password Reuse Prohibited</td>
<td></td>
</tr>
<tr>
<td>Prohibited from using previous 12 passwords</td>
<td>Prohibited from using only previous 4 passwords</td>
</tr>
<tr>
<td>D. Expiration of Passwords</td>
<td></td>
</tr>
<tr>
<td>Password required to be changed every 30 days</td>
<td>Password not required to be changed every 30 days</td>
</tr>
<tr>
<td>E. Password Required For Each Logon ID</td>
<td>Password not required for each logon ID</td>
</tr>
</tbody>
</table>
A. According to the Pinellas County Information Security Policy, revised October 2005:

"2. Difficult-to-Guess Passwords Required - Secure passwords contain both letters and numbers, along with symbols if the system permits this. These rules should be automatically enforced if and when the security technology of a particular system permits. Users must use difficult-to-guess passwords on systems that do not automatically generate appropriate passwords. A difficult-to-guess password is one which does not consist of one type of character, and which does not appear in any dictionary. For example, a password with all letters or all numbers would not be appropriate. Common character sequences such as "123456" also must not be employed. Personal details such as a spouse's name, license plate number, social security number, and birthday must not be used unless accompanied by additional unrelated characters."

The Clerk's Office-Wide Policies and Procedures 2006, Chapter 9 Technology Policy states:

"4. Passwords should contain letters and numbers, and symbols if the system permits."

The Difficult-to-Guess Passwords’ Policy requirements are not met with the current GSO settings. Passwords do not require an alphabetic character, user's logon ID as password is allowed, passwords do not require a numeric character, passwords that are only numeric are allowed, passwords are not required to contain either a national or user-defined character between the first and last position and passwords are not checked for reserved word prefixes.

B. The Pinellas County Information Security Policy also states:

"3. Cyclical Passwords Prohibited - Users are prohibited from constructing fixed passwords by combining a set of characters that do not change, with a set of characters that predictably change. In these prohibited passwords, characters which change are typically based on the month, a department, a project, or some other easily-guessed factor. For example, users must not employ passwords like 'X34JAN" in January, "X34FEB" in February, etc."

The Clerk's Office-Wide Policies and Procedures 2006, Chapter 9 Technology Policy states:

"6. Sequential passwords ("Password01", "Password02", etc.) are not permitted."

GSO settings are not in place to help enforce the Cyclical Passwords Prohibited policy requirements. No password similarity checking is performed and passwords are not checked for reserved word prefixes.

C. The Pinellas County Information Security Policy also states:
"4. Password Reuse Prohibited - Users may not re-use a password unless at least 12 months has passed since the password was last used. Systems with the capability to enforce this automatically should have this ability turned on."

The Clerk's Office-Wide Policies and Procedures 2006, Chapter 9 Technology Policy states:

"5. Passwords on critical systems are to be changed every 30 days, and may not be re-used for a period of one year. Non-critical systems shall be designated by management."

The Password Reuse Prohibited Policy requirements are not met with the current GSO settings. Users are only prohibited from using the four passwords.

D. The Pinellas County Information Security Policy also states:

"8. Expiration of Passwords - Passwords should be changed periodically according to Agency policy."

The Clerk's Office-Wide Policies and Procedures 2006, Chapter 9 Technology Policy states:

"5. Passwords on critical systems are to be changed every 30 days, and may not be re-used for a period of one year. Non-critical systems shall be designated by management."

The Expiration of Passwords Policy requirements ("Passwords on critical systems are to be changed every 30 days") are not met with the current GSO settings. The PSWDMAX day's value should be set to an appropriate maximum value to apply on a global basis. Individual agencies have the option of overriding the global value for individuals.

E. Best practices require that a password be required for each logon ID. Requiring a password for each logon ID also supports the Pinellas County Information Security Policy's purpose to:

1. Protect information technology;
2. Minimize liability and determine acceptable risk related to information and information technology;
3. Assign responsibility and roles for information and information technology.

The Pinellas County Information Security Policy's purpose is not met with the current GSO setting. Passwords are not required for all logon ID's when a logon ID is inserted or a change command is issued for a logon ID to remove the STC or RESTRICT privilege.

Since management did not set the Global System Options to enforce these password policies, passwords chosen by Mainframe users may not be strong and easily compromised. Weak passwords leave critical data and resources vulnerable to unauthorized access. The reliability,
appropriate confidentiality, and availability of critical information are at risk, which can lead to operational and financial consequences, which can have a negative impact on the County.

Recommendation:

Management implement practices to support the Pinellas County Information Security Policy for password controls. The Global System Options should be changed for password controls to enforce difficult-to-guess passwords’ requirement, prohibit cyclical passwords, prohibit password reuse, require the expiration of passwords and require a password for all logon ID’s.

Status:

Partially implemented. Several Global System Options changes were completed in February 2009 with the approval of the Pinellas County’s Security Panel. However, several Pinellas County Information Security Policy requirements are still not met with the current GSO settings as detailed below. This results in the risk that passwords chosen by Mainframe users may not be strong and could easily be compromised.

<table>
<thead>
<tr>
<th>POLICY</th>
<th>Global System Options Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Difficult-to-Guess</td>
<td>Implementated</td>
</tr>
<tr>
<td>Alphabetic character required</td>
<td></td>
</tr>
<tr>
<td>User’s logon ID as password prohibited</td>
<td>Implementated</td>
</tr>
<tr>
<td>Numeric character required</td>
<td>Implemented</td>
</tr>
<tr>
<td>Alpha-numeric passwords required</td>
<td>Implemented</td>
</tr>
<tr>
<td>Character required</td>
<td>Not Implementated</td>
</tr>
<tr>
<td>Reserved word prefixes prohibited</td>
<td>Not Implementated</td>
</tr>
<tr>
<td>B. Cyclical Passwords Prohibited</td>
<td></td>
</tr>
<tr>
<td>Similarity checking performed</td>
<td>Not Implemented</td>
</tr>
<tr>
<td>Reserved word prefixes prohibited</td>
<td>Not Implemented</td>
</tr>
<tr>
<td>C. Password Reuse Prohibited</td>
<td></td>
</tr>
<tr>
<td>Prohibited from using previous 12 passwords</td>
<td>Partially Implemented: Prohibited from using only previous 4 passwords</td>
</tr>
</tbody>
</table>
Status of Recommendations  
Follow – Up Audit of ACF2 Mainframe Security Software

<table>
<thead>
<tr>
<th>POLICY</th>
<th>Global System Options Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>D. Expiration of Passwords</td>
<td></td>
</tr>
<tr>
<td>Password required to be changed every 30 days</td>
<td>Implemented</td>
</tr>
<tr>
<td>E. Password Required For Each Logon ID</td>
<td>Implemented</td>
</tr>
</tbody>
</table>

Management Response:

They are currently working with the vendor to implement enhancements to the current GSO setting that will align closer with the Pinellas County Information Security Policy.

3. No Systematic Process Exists For Review Of ACF2 Logging And Violation Reports.

ACF2 logging and violation reports are not actively reviewed on a regular basis by management (see Opportunity for Improvement No. 4). There is no procedure for reviewing the reports and following up on potential problems; the Tech Support staff responsible for ACF2 administration review the reports a couple of times a week and only investigate violations if there are a few per user. In addition, there is no set threshold for how many violations constitute an investigation. Due to the sheer volume of these reports (approximately 500 to over 1,000 pages daily), a process needs to be adopted for efficiently reviewing the report to focus on potential problems. Logging should be reviewed if there is an indication of potential abuse of privileges and to ensure periodically that events that trigger logging were completed as planned. Violations that meet the threshold established should be closely reviewed as they are a result of failed attempts to access information. Management should use this information as a possible indication of problems in ACF2 administration and its effectiveness, and to determine if there is a breach of security.

The need for written procedures for recognizing and categorizing violations was not recognized by staff. Written policies and procedures provide guidance that is necessary to properly and consistently carry out departmental activities at a required level of quality. The establishment of the policies and procedures provides the opportunity for management to ensure that adequate process/external controls have been established. It is management’s responsibility to establish written internal procedures covering key department processes. The procedures should be in sufficient detail to provide standard performance criteria and reduce the risk of misunderstanding and/or unauthorized deviations that could cause processing errors. The development of the procedures could prevent the establishment of unnecessary controls or steps that negatively affect process productivity. The procedures also support the cross-training and back-up for key staff functions.
Abuse of ACF2 privileges, such as NON-CNCL, READALL or SECURITY, attempted hacking and breach of security, may be overlooked. ACF2 administration effectiveness cannot be adequately evaluated if the reports, which contain potential indications of problems, are not reviewed systematically. Specific guidance needs to be established outlining the frequency of review, thresholds for violation investigation and escalation procedures to process the report in the most efficient and effective manner.

**Recommendation:**

Management review ACF2 logging and violation reports on a periodic basis. We recommend management develop guidelines as to what constitutes a problem and procedures for appropriate review.

**Status:**

Partially implemented. In 2009, the Security Group tried converting this report to an automated review using 'RSA Envision' software. This process was not successful. Management is reviewing the reports manually on a regular basis (daily); however, there is still a risk of inefficiency and possible overlooked problems since specific thresholds for violation investigation and escalation procedures to process the report still have not been drafted.

4. Changes To The ACF2 Configuration Are Not Properly Reviewed And Authorized.

There is no set authorization and review process used for ACF2 user ID modifications, rule ID modifications and information storage updates. All changes should go through the Customer Support Center (CSC) ticket process for change management; however, our review found that not all modifications and updates are documented. We took a sample of changes from the User-ID Modification Log, Rule-ID Modification Log and Information Storage Update Log to determine if changes to the ACF2 database are properly reviewed and authorized. Most changes did not have a ticket from the CSC as supporting documentation. The ticket acts as a change control to ensure only authorized changes are made and provides documentation for the change. According to management, most user ID modifications and information storage updates are done as requested by two individuals in the Tech Support Group responsible for Mainframe security. Any tickets generated or e-mail requests are saved, but many requests are verbal. According to management, there is usually a ticket for rule ID modifications; however, our review of four changes made over a period of four consecutive days found that only two of the four changes had a supporting ticket.

We also evaluated the review of the User-ID Modification, Rule-ID Modification, Information Storage Update, Restricted User-ID Job and Invalid Password Authority Logs to determine if the reports were reviewed on a periodic basis and appropriate follow-up actions taken. There is no set procedure or time-table for review of these ACF2 change reports. The Tech Support Staff responsible for ACF2 keeps about a year's worth of the Rule-ID Modification and
Information Storage Update Logs. The other Logs are not reviewed consistently unless staff is looking for something specific (see Opportunity for Improvement No. 3).

According to ITIL Version 2, 8.1 Goal of Change Management:

"The goal of the Change Management process is to ensure that standardized methods and procedures are used for efficient and prompt handling of all Changes, in order to minimize the impact of Change-related Incidents upon service quality, and consequently to improve the day-to-day operations of the organization."

This is supported by the IT Change Management High Level Process, Version one, which states the goal of Change Management under 1.1. Goal & Objective as:

"To manage and control Changes to the Pinellas County production environment with the least possible risk of service level disruption."

The IT Change Management Policy Document, Version one states:

"The following must be adhered to by any staff or department/agency making changes to production systems managed by Pinellas County IT.

1. All computer and communications systems used for (automated) production processing must employ a formal change management procedure which is used to ensure only authorized changes are made.

2. The change management procedure must be used for all changes to software, hardware, communications networks, and related procedures (documentation).

3. Changes (RFCs) classified as "Standard" are not required to exercise the Change Management Process or come before the Change Manager, however they must follow appropriate communication and testing procedures. Standard changes only qualify for individuals with the appropriate skills and experience in order to minimize the risk associated with the change. If uncertain whether a change may be considered as Standard, the individual must check with the Change Manager or a member of the Change Advisory Board (CAB) prior to implementing."

Management is circumventing the change control process for ACF2 database changes and has not determined what types of changes can be classified as standard. Not following a standardized process for handling changes can result in higher risk exposure, which can have a negative impact on or disrupt ACF2 users. Without utilizing a structured approach, unauthorized changes can occur, changes may be handled inefficiently and errors can be made. In addition, traceability of changes is compromised without adequate documentation.
Recommendation:

Management create a standard procedure for routine changes to the ACF2 database in alignment with the IT Change Management Process and approved by the Change Manager or Change Advisory Board. We recommend the Change Management Process utilized by Information Technology be followed for all other ACF2 database changes. We recommend a periodic review by management or an independent party be conducted to ensure changes to the databases are authorized (see Opportunity for Improvement No. 3).

Status:

Implemented. The Mainframe team utilizes the industry standards of ITIL Foundation for Change Management within BTS. These standards, policies and procedures are followed for tracking and logging ACF2 changes. Each change is reviewed by an approval authority consisting of BTS Management.

5. No Formal Written Policies And Procedures Have Been Established For Maintaining ACF2 Software.

ACF2 software maintenance is performed by the IT Tech Support Group as needed with no defined process. The department has not developed formal written policies and procedures covering the processes for applying system maintenance, reviewing and modifying system options and applying program fixes to the mainframe security software. Management stated that ACF2 system maintenance is done on an as needed basis and usually occurs on the weekends since the Mainframe must be bought down. ACF2 system options are not routinely reviewed and modifications are made as needed. Application of ACF2 program fixes issued by Computer Associates to limit integrity exposures are performed by a Mainframe Lead Systems Programmer as they are received. These current verbal procedures are outside the normal process for configuration, change and release management and have internal control weakness that can affect the department operations.

The goals of configuration, change and release management all rely on set policies and procedures to guide the processes. ITIL Version 2, Service Support, 7.3.6 Configuration baseline states:

"A configuration baseline is the configuration of a product or system established at a specific point in time, which captures both the structure and details of a configuration. It serves as reference for further activities... A configuration baseline is used to assemble all relevant components in readiness for a Change or Release, and to provide the basis for a configuration audit and regression, e.g. after a Change. The Configuration Management system should be able to save, protect and report on a configuration baseline, its contents and documentation."

ITIL Version 2, Service Support 8.1 Goal of Change Management states:
"The goal of the Change management process is to ensure that standardized methods and procedures are used for efficient and prompt handling of all Changes, in order to minimize the impact of Change-related Incidents upon service quality, and consequently to improve the day-to-day operations of the organization."

ITIL Version 2, Service Support 9.1 Goal of Release Management states:

"The focus of Release Management is the protection of the live environment and its services through the use of formal procedures and checks."

As discussed in Opportunity for Improvement No. 3, written policies and procedures provide guidance that is necessary to properly and consistently carry out departmental activities at a required level of quality. According to COBIT 4.0, DS13 Manage Operations states:

"Complete and accurate processing of data requires effective management of data processing and maintenance of hardware. This process includes defining operations’ policies and procedures for effective management of scheduled processing, protection of sensitive output, monitoring infrastructure and preventative maintenance of hardware. Effective operations management helps maintain data integrity and reduces business delays and IT operating costs."

The need for written policies and procedures was not recognized by staff nor are they included in the standard configuration, change and release management processes for ACF2 maintenance. Lack of policies and procedures can lead to ACF2 system maintenance processes not being handled in a standardized manner. A defined approach for system maintenance, configuration of system options and applying program fixes in an efficient and effective manner mitigates the risks of staff members not knowing how to perform critical tasks, disruptions in production processing, undocumented changes, critical maintenance or installation of program fixes not performed timely and insufficient control over emergency changes.

Recommendation:

Management develop written policies and procedures, which will provide the necessary information to keep the process current and accurate. Cross-training should be provided to ensure that a second appropriate staff member could carry out the responsibilities of the function. ACF2 software maintenance should go through the normal configuration, change and release management processes. One method would be to create a version control procedure in which changes to the ACF2 software are tracked. The version control document should include pertinent information related to the change, including version date, version number, reason for version change, requestor and approver.
Status:

Implemented. Formal written documentation for maintaining the ACF2 product was written in 2009. The documentation is accessible by the mainframe system administrators via a secured shared directory. The ACF2 maintenance and version control is managed through the ITIL Foundation Change Management process. The documentation and maintenance process is kept current.
DIVISION OF INSPECTOR GENERAL

KEN BURKE, CPA
CLERK OF THE CIRCUIT COURT
PINELLAS COUNTY, FLORIDA

Write: Fraud Hotline
Public Integrity Unit
Division of Inspector General
400 Cleveland St., 4th floor
Clearwater, FL 33755-4041

Phone: (727) 453-3728
Fax: (727) 464-8386

E-Mail: fraudhotline@pinellascounty.org
Internet: www.mypinellasclerk.org

Accredited Office of Inspector General
by the Commission for Florida Law Enforcement Accreditation