Fairfax County Internal Audit Office

Department of Family Services
Department of Administration for Human Services
Harmony System Audit
Final Report

September 2006

"promoting efficient & effective local government"

Executive Summary

The Harmony system was implemented by Fairfax County Human Services in 2000 to replace the old Mainframe based system VUWRS (Virginia Uniform Welfare Reporting System). Average payments of $43 million per year were processed on the Harmony system between its implementation through the end of FY 2004. Over 80% of those payments, about $35 million, were made under the Comprehensive Services Act program and the remaining was divided between the Adult and Aging and the Self Sufficiency programs. Harmony's financial and vendor management is performed by the Department of Administration for Human Services' Finance Office which works independently of the county's Department of Finance (DOF) and Department of Purchasing and Supply Management (DPSM).

Our audit found that access to the Harmony system did not incorporate proper separation of duties and the "*least privilege"* concept which is required by the county's Information Technology Security Policy PM 70-05. Access request forms were not maintained and shared user accounts were allowed. Moreover, data in the system were modified without documented authorizations. Even though Harmony provides various reports and audit logs of user activities and system events, management review and monitoring were not performed. The above conditions have contributed to the following areas of weakness:

- Opportunity for users to make unauthorized changes to critical application data
- Violation of the county's Information Technology Security Policy

Certain system and vendor related information has been omitted from general disclosure. This information would, if disclosed, subject the county to potential financial and system vulnerabilities.

Scope and Objectives

This audit was performed as part of our fiscal year 2006 Annual Audit Plan and was conducted in accordance with generally accepted government auditing standards. The audit covered the period of July 2004 through June 2005 and was conducted to determine that the Department of Family Services (DFS) and the Department of Administration for Human Services (DAHS) have put procedures in place to ensure the following objectives were achieved within the Harmony system:

- Access controls and management trail information were adequate
- Payments to vendors were authorized and supporting documents maintained
- System administrator capabilities were monitored

This audit was not intended to examine or report on previously identified issues that were found as part of either the financial process review performed by the Department of Finance or the investigation of the Harmony system performed by the Internal Audit Office. The issues that were reported on as part of the above reviews included:

- Harmony system payment process including internal controls and separation of duties
- Security and controls over the interface to FAMIS
- Controls to ensure proper reporting of 1099 payments and controls to prevent duplicate payments

Furthermore, our audit did not include a review of the general controls environment, including the security and controls over the SQL Server database in which the Harmony application data is stored. The effect of this scope limitation is that if weaknesses exist in the general controls environment, this could have a negative impact on the integrity of the application data.

Methodology

Our audit approach included a review of the Harmony application controls with emphasis on the access controls and separation of duties, the adequacy of management trail information including the monitoring of the system administrator's capabilities. We assessed compliance with the county's Information Technology Security Policy PM 70-05 with respect to account management, back-up and contingency plans, business continuity and disaster recovery plans. We also performed audit steps designed to help us detect indications of fraud and illegal acts.

The Fairfax County Internal Audit Office is free from organizational impairments to independence in our reporting as defined by Government Auditing Standards. We report directly and are accountable to the county executive. Organizationally, we are outside the staff or line management function of the units that we audit. We report the results of our audits to the county executive and the Board of Supervisors, and reports are available to the public.

Findings, Recommendations, and Management Response

1. Access Controls and Separation of Duties

User account permissions were granted that would allow for a single user to add new vendors, process invoices and prepare checks for payment. Seventeen of the twenty-five user profiles that we tested had access levels that prevented separation of duties. Proper separation of duties dictates that tasks and associated privileges for a specific business process be disseminated among multiple users. The likelihood of fraud and errors are increased without proper separation of duties within the user account management process.

Recommendation: We recommend that user access to the Harmony system's resources be limited to that set of privileges necessary for user to perform their job. In addition, access control should enforce proper separation of duties so that no one employee has the access and privileges associated with the entire payment process within Harmony.

Management Response: Both the client server and the web versions of Harmony have security features allowing for regulation of access and separation of duties.

Individual and group profiles have been modified so that users only have access to functions required of their position. No position has access to the entire payment process with the exception of the system administrators.

There are three components of the payment process in Harmony. One is the consumer record, the second is the provider record and the third is the purchase order/invoice processing. Program staff are the only ones able to create and modify consumer records. CSA/DFS Finance team staff are the only group allowed to create purchase orders and make payments. Staff who make payments can not create or modify provider records. Staff who manage providers can not make payments or create checks. Staff that create checks do not make payments or modify providers.

A thorough review and update of all profiles will be done so that these rules are verified to be in place. The anticipated completion date is September 30, 2006.

2. Access Request and Approval Forms

Access request and approval forms were not maintained for the sample of twenty-two users that we tested. In fact, access request and approval forms for all users from the time of the implementation of the Harmony system had been lost according to the Harmony system administrator. PM 70-05 states that every user account should have an associated request and approval for the level of access granted. Among other information, these forms should document management's explanation as to the appropriateness of the access level being requested for the users. Management approval of the level of user access granted cannot be verified without documented access request forms.

Recommendation: We recommend that new user access request and approval forms be completed by the appropriate management for all system users. In addition, the Harmony system administrator should reconcile the access level indicated in the newly obtained approval forms to the access level currently granted in the Harmony system to the above users.

Management Response: Access request and approval forms for the twenty-two employees used during internal audit's testing will be created no later than September 30, 2006. DFS will further review all (160+) current Web Harmony user accounts to ensure proper access forms are in user files. DFS is also planning to re-create new user access and approval forms for all Client Server Harmony users as they will transition to Web Harmony by the end of current fiscal year.

While we currently have access forms in place, we are introducing additional improvement steps to ensure all future users will have proper access forms in file. DFS's new access and approval form will require a business as well as DFS IT manager's signature prior to granting access to Harmony.

3. Account Management – Shared Accounts

We found a total of forty-three shared user accounts where users were able to perform various tasks including update. PM 70-05 requires that all accounts be uniquely identifiable using the assigned user name. This provides accountability by associating tasks performed with the user name that performed it. By allowing user accounts to be shared by two or more users, tasks performed could not be associated to the individual users thereby preventing accountability.

Recommendation: We recommend that all shared accounts be deleted from the system and replaced with new accounts that are assigned to uniquely identifiable users.

Management Response: Shared accounts were originally setup for some users to accommodate shared cases as some business areas provide services and manage cases as a unit. We are currently de-activating shared accounts and assigning individual accounts to each user.

4. Changes to the Vendor File Not Documented

Vendor addresses and their service price rates were changed in the vendor file without documented authorization. Internal control procedures of DAHS Finance require authorization by the area manager or a designated staff before the vendor file can be modified. None of the twenty-two records tested had such authorization. Without the authorization form that shows the signature, date and the reason for the vendor file changes, unauthorized changes to the vendor file might go unnoticed.

Recommendation: DAHS/DFS management has already implemented controls to ensure authorization for changes to the vendor file are documented for future management review and/or audits. Thus, no further steps are required for management to respond to this finding.

Management Response: No further response required.

5. Review of Management Trail and Monitoring of System Activities

There was no management review process to monitor the activities of the system administrators and special users (i.e. users who can approve invoices, and prepare checks). Currently, there are two system administrators and seven special users. These users had unlimited access to incompatible functions that hinder proper separation of duties. Unauthorized or erroneous changes to vendor information (i.e. vendor address change thereby sending payment checks to such address) can go unnoticed without a management review process.

Recommendation: We recommend that a management review and monitoring process be implemented based on assessment of potential unauthorized alteration/disclosure, and/or loss of the data processed and stored within Harmony. Emphasis should be placed on the system areas that pose the highest risk such as the activities of the system administrators and special users.

Management Response: DFS will work with DIT and/or Harmony information system to develop a report that will capture Harmony system administrator's as well as business administrators' special activities in Harmony. The report will be reviewed and approved by DFS IT manager on a monthly basis and reviewed by the Director or his designee annually. We anticipate completion of a draft report for review by September 30, 2006.