Fairfax County Internal Audit Office

Department of Finance
FOCUS Electronic Payments Audit
Final Report

March 2015

"promoting efficient & effective local government"

Executive Summary

The Department of Finance (DOF) uses the Fairfax County Unified System (FOCUS) to set up and maintain vendor files, generate electronic payment files, and transmit payment files to the county's financial institution, Bank of America (BOA). BOA sends the payments to vendors via ACH, check or wire transfer based on the instructions provided by payment files. In FY 2014, DOF made approximately 73,000 electronic payment transactions through FOCUS worth $2.26 billion.

Our audit found that there were controls in place to ensure payment files were generated timely and accurately in FOCUS. Payment files were encrypted during transmission, and the encrypted payment files were transferred to the BOA server via Secured File Transfer Protocol (SFTP). We also verified that reconciliation was performed to ensure payment files were completely and accurately sent to BOA. We determined controls were in place for vendor file setup and maintenance, and segregation of duties control was implemented between data entry and transaction posting and approval. In addition, we found that FOCUS can generate and maintain audit trail data to determine how, when, and by whom specific actions were taken. However, during our audit, we noted that the DOF had previously identified that controls over two of their user roles could be strengthened by splitting them into three distinct roles, and reassigning users into these new roles. DOF is currently working with FBSG and DIT to setup the new user roles in FOCUS.

Scope and Objectives

This audit was performed as part of our fiscal year 2014 Annual Audit Plan and was conducted 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. This audit covered the period of January 1, 2014, through August 30, 2014, and our audit objectives were to:

- Review the contract and service level agreement between BOA and the DOF to ensure that proper documentation exists for all relationships, and responsibilities were clearly spelled out.
- Determine whether the data transmission between BOA and the county was secure, and reconciliations were performed to verify data completeness.
- Determine the integrity of vendor files, and whether payment files were generated timely, accurately and completely in FOCUS.
- Determine whether BOA and the DOF have a Business Contingency Plan (BCP) to continue electronic payment activities in the event of interruption.
- Verify whether protections were in place to prevent unauthorized modification, and to prevent vendor information from being disclosed without their consent.

Methodology

Our audit approach included a review and analysis of internal controls over the FOCUS electronic payments processing. We interviewed appropriate employees to understand the system functions, vendor file setup and maintenance, payment files generation, data transmission to BOA and the reconciliation process. We reviewed the contract between the county and BOA; observed employees' work functions; determined whether the data transmission between the county and BOA was secure; tested payment files generation, and the reconciliation process after data transmission; and verified user list accuracy on a sample basis.

Findings, Recommendations, and Management Response

1. FOCUS Accounts Payable Users' Access Rights

During our audit, the Internal Audit Office (IAO) requested the FOCUS Business Support Group (FBSG) generate lists of users with access to run payment proposal (transaction code F110), to confirm a change of vendor information (transaction code fk08), and to block/unblock vendor payments (transaction code xk05). We noted that DOF had 16 users with access to run F110 in FOCUS. Based on their current job responsibilities, not all of these users needed to have access rights to F110. Prior to this audit, DOF reviewed and evaluated the user lists, and determined it was necessary to split the 16 users from two roles into three distinct roles, and permit only seven of these users to have access rights to F110. Additionally, DOF found one user should be removed from the vendor update access rights. IAO also learned DOF was working with FBSG and DIT prior to the start of our audit and continues discussions to setup the new user roles in FOCUS. Once established, these roles will be tested by both FBSG and DOF staff. After testing is complete, the new user roles will be setup in the production environment.

Fairfax County Information Technology Security Policy 70-05.01 states that the owner of information assets shall implement procedures and safeguards to ensure that access to Fairfax County Government information is made available only to those who have the right to such access. The concept of "Least Privilege" i.e., providing only those privileges necessary to perform one's job function, will be used to insure the security of networks, computer systems and Fairfax County Government data.

Although there were compensating controls to mitigate the financial risk for this particular instance, a periodic review of user access through their roles increases the effectiveness of user roles setup, and reduces the risk of fraud or error through inappropriate access.

Recommendation: We recommend that DOF work with FBSG and DIT to periodically review the FOCUS system Accounts Payable user roles to ensure they are set up to only assign users access rights necessary to perform their job functions. Additionally, DOF should ensure the user roles change described above is implemented in the production environment.

Management Response: These roles were “Elevated Privilege” Roles (as defined by the DIT Information Security Office), and any request to be granted access to these roles now requires review and approval by designated DOF and FBSG staff. We will continue to work with both FBSG and DIT to ensure users’ accounts payable roles are in line with job functions. Management has anticipated completing this action by May 15, 2015.