Fairfax County Internal Audit Office

Department of Finance
Treasury Workstation Application Audit
Final Report

January 2008

"promoting efficient & effective local government"

Executive Summary

The Treasury Workstation (TWS) application is used by the Investment and Cash Management (ICM) Division of the Department of Finance (DOF) to manage what is currently $2.2 billion in short term investments. It is a commercial off-the-shelf menu-driven computer application owned by SunGard, Inc. DOF evaluated controls per a review contracted through the external accounting firm, KPMG, for the initial installation of Treasury Workstation in 2003. This review was used to implement a number of significant internal control improvements. The TWS is not used to carry out investment transactions. Rather, it is a repository of investment data. The county uses the product to:

- Electronically retrieve bank information
- Record cash, investment, and debt transactions
- Reconcile system balances with bank balances
- Display net cash position at any time
- Review consequences of future transactions on the net cash position
- Print detail and summary reports
- Mark transactions for entry into general ledger system.

In our audit of the Treasury Workstation application, we found that overall, the application system controls were in place and functioning, and county investment data was entered into the TWS system accurately and completely. Separation of duties among staff of the ICM division of DOF was adequate and physical safeguards were in place. However, we noted areas where internal controls could be strengthened in regard to secure access to the application and audit trail functionality. We found that:

- Compliance with the county's Information Technology Security Policy 70-05.01 related to access controls and audit trail requirements needed to be strengthened. Password access allowed unlimited access attempts without a lock-out feature.
- System administrator monitoring was not as effective as it should be. The system changes carried out by the system administrator were not recorded in the audit trail data.
- The frequency of backups were in need of review by DOF to determine that DIT default backup parameters are sufficient for the TWS data.

The level of risk associated with these inadequacies was not as high as it would be if this application was used as a transaction processor. Since it is functioning only as a data repository for investment information, the level of risk is lower. Should management wish to use this application as a transaction processor in the future, the issues identified in this audit would be considered significant control weaknesses.

Scope and Objectives

This audit was performed as part of our fiscal year 2007 Annual Audit Plan and was conducted in accordance with generally accepted government auditing standards. The purpose of this audit was to evaluate the system controls for the application. This included

an examination of the system input, processing, security, reporting capabilities, data safeguards, online access, management transaction trails, and separation of duties.

The objectives of this audit were to determine that:

- Access controls were adequate to prevent unauthorized access to financial data
- Functional transaction categories were separate and distinct
- Reports produced were complete and accurate
- Adequate safeguards were in place to prevent lost, missing, or stolen funds
- Audit trail information was adequate
- System administrator capabilities were appropriately assigned and monitored
- Sufficient controls were in place over the system output
- Adequate backup procedures were in place, tested, and validated

This audit did not examine the manual controls used by the Department of Finance to control risk in financial transactions, nor were network controls and other applications (MS Access) evaluated.

As part of this audit, we followed up on the status of the 22 recommendations made by the external firm, KPMG, in 2003 during the implementation of the application. Five recommendations remain outstanding as follows:

- Trading desk paper was not being properly shredded or secured
- Audit trail reports and breach reports were not regularly produced and reviewed
- MS Access was used to extract sensitive information from TWS
- The TWS operator had the ability to change the status of a wire transfer
- The TWS operator had the ability to change sensitive information on previously processed transactions.

The first recommendation is included in the findings from this audit. The second recommendation is still outstanding. The last three items were outside the scope of this audit because the TWS application is not used to process the effected transactions.

Methodology

Our audit approach included reviewing the applicable system documentation, and interviewing management and staff of the ICM Division to obtain an understanding of the requirements for financial and programmatic reporting, document retention, and application security for the TWS application. The daily process of making short term investments, of which the TWS is a part, was observed from beginning to end. Staff outside of the ICM who had access to the data was also interviewed.

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. Audit Trail Records

There was no audit trail of changes made by the system administrator, nor was there evidence of complete audit log information on changes made by users. The audit trail report from the application contained only date, userid, and transaction number. There was no before and after image of the record contents in the audit trail information.

The presence of a thorough audit trail can assist management in accomplishing security objectives including detecting violations, reconstructing events, and resolving application processing problems. The lack of a trail of administrative changes and insufficient data for user changes leaves the county vulnerable to possible inaccurate data and potential exposure to error or fraud.

Recommendation: Any change to the application or database made by the system administrator or user should create a view-only audit trail record containing the date and time, user id, and before and after values for changed fields. We recommend that an audit trail be maintained of all changes made in the application by the system administrator and users. The most recent version of the TWS application software, version 8.0, has enhanced audit functionality which would allow for a more thorough audit trail implementation.

Management Response: The Department of Finance has created a Systems Administrator Log to record any and all changes to the application and users' access/entitlements. DOF has contacted Sungard regarding audit trail enhancements in more current versions of the software. In TWS 8.0, the system includes a full audit trail of changes made to user profiles. Where the system's audit trail is inadequate to record specifics of any changes made in recorded transactions, DOF will maintain a log for this purpose. TWS 8.0 will be installed as promptly as feasible. Anticipated completion date is March 15, 2008.

2. Disposal of Sensitive Hardcopy Output

Hardcopy reports generated by TWS containing bank account numbers were not being shredded. Any output containing confidential or sensitive information should be shredded or destroyed according to the county's IT Security Policy.

All hardcopy output was deposited in a container supplied by Fairfax County's recycle program. Account numbers could be used to potentially gain access to county financial information and therefore should be considered sensitive information.

Recommendation: All TWS hardcopy output containing bank account numbers should be shredded or otherwise destroyed in a way which prevents access to bank account numbers.

Management Response: All hardcopy TWS output, along with all other excess sensitive ICM material, are now being shredded.

3. Password Security Attempts

The password logic in the TWS application allowed the user three attempts to enter his/her password then wait a short period before allowing additional attempts. This substantially decreased the effectiveness of the control established by the password usage requirement.

The version of the TWS software which the county was using is coded to allow this condition. The vendor has changed the logic in version 8.0 of the product to no longer allow more than three attempts at password entry. The level of risk associated with this control weakness is lower because this application is not being used to process transactions.

Recommendation: If at some time in the future the ICM office considers usage of this application to process transactions, they should plan to upgrade to version 8.0 of the TWS to take advantage of the tighter control over access by limiting the number password attempts allowed.

Management Response: DOF will be installing TWS 8.0 which has enhanced password controls. The vendor advises that allowing multiple failed attempts has been corrected. In addition, TWS 8.0 has the ability to connect to an NT network User ID and authenticate against the network password. DOF will explore this enhancement. The anticipated completion date is April 1, 2008.

4. TWS Data Backups

The frequency of the TWS data backups and the amount of time those backups were being retained were established by the Department of Information Technology (DIT) as defaults. DOF did not verify that the backup frequency and retention periods for TWS data were sufficient.

The county's IT Security Policy requires all applications data to be backed up according to a documented plan coordinated with DIT.

The default frequency and retention of TWS data may not be adequate to protect this information and its recoverability in the event of a system failure. Depending on the recoverability of the data and software, and the length of the disaster or outage, the impact on the county could be significant.

Recommendation: We recommend that DOF evaluate the current backup practices in place for TWS data and determine whether adjustments are necessary. This evaluation of data backup provisions should result in a documented agreement between DOF and DIT for the TWS applications data.

Management Response: DOF has verified that TWS data is backed up daily. As recommended, this will be documented in a written agreement with DIT following the upgrade to version 8.0. The anticipated completion date is April 1, 2008.

Other Audit Observation

There was no documented recovery plan for the TWS application. The TWS is not considered a category one function in the DOF continuity of operations plan (COOP). However, work has been done to put in place the components necessary to continue to monitor investments if the application and/or ICM staff were not available for some period of time. The ICM has a laptop stored onsite on which the application is loaded. We recommend that the laptop or laptops be stored offsite.