



# Fairfax County Internal Audit Office

Retirement Administration Agency  
PensionGold - Application System Audit  
Final Report

March 2010

*"promoting efficient & effective local government"*

# Introduction

This report covers the audit period of January 2007 through February 2008. The Fairfax County Retirement Administration Agency (RAA) administers three separate defined benefit retirement systems: Employees', Police Officers', and Uniformed. RAA also administers the retirement payroll function for certain employees of the Fairfax County Public Schools (FCPS) with a retirement payroll of approximately \$3.3 million; however, the scope of this audit did not include FCPS members. The total population of county employees on the PensionGold system as of February 29, 2008, was 16,743, which included both active (11,973) and retired (4,770) members. These figures do not include employees who left the system but have service credit. Active members contributing to the retirement pension plan included the Employees' Retirement System consisting of slightly more than 8,600 employees. The Police Officers' Retirement System consisted of 1,367 members and is limited to sworn officers in the Fairfax County Police Department, while there were 1,938 members in the Fairfax County Uniformed Retirement System, which includes all uniformed officers in Fairfax County's Fire and Rescue Department, Sheriff's Department, and Department of Animal Control. The monthly payroll for county retirees was approximately \$14 million, which includes payment to the following retirees: regular retirees, duty disability, non-duty disability, severe duty disability, automatic payments to dependents of police upon death, and service retirements as well as survivorship.

RAA converted to the PensionGold Application System as of January 1, 2007. This system is used to manage over 24,000 active and retiree members from both the county and FCPS.

## Executive Summary

Our audit focused on controls over the PensionGold Application System used to calculate employee pensions and manage retirement administration functions including enrollment, terminations and refunds, employment history, benefit payments, member statements, and query/reporting. The implementation of PensionGold was accomplished in a compressed time frame and improved many system weaknesses from the previous systems. Our review did not focus on manual calculations; however, we found that RAA was using a thorough manual process to reexamine all data used in the calculation of employee retirement benefits. This was done to ensure the accuracy of the benefits calculations.

We found that there were some inconsistencies in data elements between other system reports, the PensionGold application, and/or manual calculations. However, RAA management and staff have taken extra steps to validate employee pension data prior to calculating employee pension benefits. There were instances of compensating controls in that manual calculations included second and third reviews. Future enhancements to the PensionGold system could provide the application with additional functionality to support/strengthen RAA's business processes and to reduce the existing number of manual work-arounds currently being used, which would more efficiently utilize the system's capabilities. While we noted a lack of certain controls and

procedures existed at the onset of the audit, RAA was taking steps to analyze and implement needed procedures.

At the start of our audit, we also found internal control weaknesses in the area of access control restrictions for the PensionGold data. While there was an audit trail feature and change report, steps needed to be taken to ensure that exception reporting, supervisory oversight, or other preventative measures were fully in place, protecting the integrity of employee data. We recognize the efforts of RAA management and staff in spending a considerable amount of time working through the initial system anomalies.

We did not identify any weakness with the calculation process. We cannot express an opinion on the integrity of the data related to calculating employee pensions, because this function, due to its complexity, was handled manually by RAA counselors with the help of some automated tools. However, there was adequate separation of duties between employees handling initial setup and collection of new members' contributions and payment of funds to retirees. The more significant issues are listed below in their respective categories with additional issues included in the detailed findings and recommendations section.

#### Controls:

- Technical Services staff had access rights to perform all functions of the PensionGold application without sufficient oversight. However, we did note that they could not set up new members on the system. This creates the risks that unauthorized activity could go undetected.
- Processes have now been put into place to review data updates made within the PensionGold system; however, at the start of our audit, there was a lack of complete oversight or monitoring of updates made to data such as beneficiary changes, address changes and deduction adjustments.

#### System Issues:

- The system did not require strong passwords or passwords be changed on a periodic basis.
- RAA could benefit from obtaining additional PensionGold exception reports to identify anomalies involving data entered on a monthly basis, such as amounts over a certain threshold.

Certain RAA operational and application data related information has been omitted from general disclosure. This information, if disclosed, would subject the county and RAA to potential operational disruptions and risks.

## Scope and Objectives

This audit was performed as part of our fiscal year 2008 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 from January 2007 through February 2008. In addition to this audit, we performed a follow-up of findings noted during a prior investigation. The results of that follow-up have been communicated in a separate memorandum.

The objectives of our audit were to determine that:

- The system input, processing, security, and reporting capabilities were effectively and efficiently managed.
- Satisfactory internal controls existed and were effective to safeguard data against misplaced, misappropriated, or embezzled funds.
- Data safeguards, on-line access, management transaction trails, and separation of duties were in place and operating satisfactorily.

## Methodology

Our audit approach included on-site visits to the Retirement Administration Agency, interviewing and observing employees' work functions, reviewing the application system as well as reviewing documentation including reports, audit logs, employment-to-date deduction calculations, and segregation of duties. Data was examined for reasonableness and samples were taken using audit software to evaluate appropriateness of audit evidence. We also performed substantial sample testing of initial hire dates, leave accrual dates, pension plan selections, pension deductions for both the employee and the county's contributions, and payment applications using audit software tools to evaluate the processes for compliance with internal controls, departmental policies and procedures as well as county policies.

## Findings, Recommendations, and Management Response

### Controls

#### 1. Access Controls

The two members of the RAA Technical Services staff and the vendor had access rights to perform all functions of the PensionGold application. We did note that they would not be able to create new members; however, they would be able to perform all other steps within a transaction process. This circumstance could negate the implementation of separation of duties designed to institute checks and balances over PensionGold processes.

Section 2.0 – Operational Policies of the county's IT Security Policy states that, "...access control shall be implemented along with procedures that stipulate and safeguard access to county information only to those with privileges necessary to perform their job function. The concept of 'least privilege' should be followed." Initial setup of the access rights for PensionGold users established system administrator status for both technical services staff as well as a generic user ID.

**Recommendation:** We recommend that RAA evaluate the access rights and reassign these capabilities to staff based on a job-related need-to-know methodology. RAA should also delete the generic user ID and create a vendor user ID that will be separately managed and the password will be updated on an agreed upon cycle. In addition, for those who do have full unlimited access rights, there should be exception reports that specifically address all transactions that they carry out in the system from a transaction perspective. This exception report should be reviewed by management on a regular schedule.

**Management Response:** RAA has thoroughly reviewed the current privileges/security settings of the technical services staff and determined how administrative functions can best be maintained with the 'least privilege' possible. Audit trail transactions for both technical services staff members are now reviewed on a regular basis. Now that PensionGold has been fully implemented, the generic user ID has been deleted.

## 2. Inactive User IDs

We found that there were user IDs with active status in the system, which needed to be removed. Access rights for PensionGold user ID XBSOHNO were still active several months after the employee had left the RAA, and user ID TRAINER was activated at the initial conversion of the application in January 2007; however, this user ID had been inactive for more than one year. We note as a mitigating factor that these two user IDs did not have county network access.

There was no evidence to indicate the user ID logs were being monitored to ensure that inactive user ID accounts were deleted from the database. If the network access were still in place, former staff could use inactive user IDs to access the system and perform unauthorized activity.

**Recommendation:** We recommend that RAA delete the inactive user IDs and monitor the user ID database on a regular basis to ensure terminated users are promptly removed from the database. The two user IDs (XBSOHNO and TRAINER) were deleted from the PensionGold database on April 23, 2008, after our discussion with RAA.

No response is needed for current inactive user IDs as management has taken steps to address this issue. The inactive user IDs were deleted after notification from Internal Audit. However, the need to monitor the user ID database on a regular basis remains as an ongoing task.

## 3. Password Criteria

While access to the PensionGold system requires that one first have network access where strong passwords are enforced, our review of password capabilities for compliance with county policy PM 70-50 identified several weaknesses. Per PensionGold setup done by RAA, passwords were not being

required to be changed by checking the “enforced” parameter at a specific time frame (60 days or 90 days) for 12 of 17 or 71% of the PensionGold user IDs. The five that had been set up with these requirements were not done as a matter of policy. The application did not enforce strong passwords (special characters or case sensitive with a minimum of 6 characters). Password changes were not required by a new user the first time an account was established.

The county’s IT Security Policy requires the following for strong passwords:

- All initial passwords should be changed,
- Passwords shall be routinely changed (at a minimum, not longer than every 90 days),
- Passwords should adhere to a minimum length of six characters,
- Passwords should adhere to a specific case sensitive format of uppercase, lowercase, and special characters,
- Passwords should not be anything that can be easily tied back to the account owner: user name, SSN, nickname, relative’s names, birth date, etc.,
- Passwords shall not be dictionary words or acronyms, and
- Password history shall be retained to prevent the reuse of a password.

By not changing the user passwords after a maximum of 90 days and not enforcing password changes the first time an account is established, there was nothing to prevent the system administrator(s) from having knowledge of the users’ passwords. In addition, by not enforcing strong passwords and not ensuring that the password format is case sensitive, both the system and the data are more vulnerable to errors, omissions, and password cracking.

**Recommendation:** We recommend that the RAA request that the vendor upgrade security in the application to support strong password requirements. In accordance with IT Security policy #70-05, this requirement in the policy should be adhered to in all newly created and system development. This should be documented in the PensionGold procedures and implemented at training sessions.

RAA has since updated the password requirements for the twelve employees that were not previously set up. However, the need to set up requirements for strong passwords, and password history retention still remain outstanding.

**Management Response:** Discussion and negotiations with the vendor have begun in regard to upgrading PensionGold to require the use of strong passwords. The vendor has proposed two solutions; however, there are significant cost factors involved. The agency is reviewing and negotiating the cost factors.

#### 4. **Edit Review**

At the onset of our audit, RAA retirement counselors could make updates to data in the PensionGold system and there would be no review by anyone of the changes made. These changes included data fields such as direct deposit

account information, beneficiaries, address changes, tax exemption information code, re-evaluation date for disabled employees, deduction adjustments, subsidiary benefits coverage, and tax code. We initially determined, via staff interviews in Business Operations and Membership Services, that no review was performed at that time.

Subsequent information advised that data review was performed on a sample basis manually from a change log generated by the system.

As stated in county ATB40070 – Processing Monetary Receipts, under paragraph Separation of Duties for Monetary Collections, departments are required to develop a system of checks and balances so that no individual person is responsible for the completion of all steps in processing monetary receipts. Such controls provide reasonable assurance that errors or irregularities will be detected in a timely manner, by others in the normal course of their duties.

**Recommendation:** We recommend that RAA management create and enforce functional oversight processes to ensure that transactions may not be independently carried out without proper and separate review.

**Management Response:** The RAA embraces the concept of “separation of duties.” To that end, staff regularly performs desk audits of processed applications. Processed applications are regularly reviewed to ensure that all necessary documents are contained in file jackets. The addition of exception reports will greatly enhance this procedure. All monetary changes are peer-reviewed and then reviewed by management.

## Documented Procedures

### 5. Disaster Recovery Plan Procedures

While it appears that RAA participated in the countywide Continuity of Operations Plan effort, additional steps were needed to ensure a complete, fully documented and approved business continuity plan for the PensionGold application, and that a thoroughly tested plan, was in place. The county’s IT Security Policy requires all essential or mission critical applications have a viable and logical business continuity plan or a disaster recovery plan.

In the case of an incident affecting the Retirement Administration Agency system, there was not a documented way to continue the operation of the retirement office. Depending on the recoverability of the data and software, and the length of the disaster or outage, the impact to county retirees could be significant.

**Recommendation:** We recommend that a business recovery plan be developed, which includes the major retirement member functions of the Retirement Administration Agency. This should take the form of written documentation detailing how to proceed using alternative tools if the PensionGold system or access to the facility is not available. At a minimum, a

disaster recovery plan should have detailed steps for preventative measures; it should be organized, staffed with responsible team members, tested for effectiveness, and be approved by management.

**Management Response:** The written Disaster Recovery Plan is being finalized. A contingency plan exists that if the system were to go down, the agency could process monthly payments with data from the previous completed month. One challenge with this is that new retirees could not be put on the payroll until the following month. If the agency were closed for a significant amount of time due to a catastrophe, the PensionGold system can now be accessed remotely by several key personnel. With the implementation of WebMember Services, the agency also has a back-up of data residing on the vendor's servers in Springfield, Illinois.

## System Issues

### 6. Exception Reports

There were few PensionGold exception reports to identify anomalies to the data that was entered on a daily basis to cover over payments. Examples of potential reports could include, but are not limited to, reports which monitor benefit payment amounts over a certain threshold, increasing amounts to a certain threshold, increasing amounts to already retired or deceased members, exceptions between the prior month and the current month, and significant differences outside of the established COLA amount, or to a limited number of individuals. Also, there was no report to identify changes in bank account numbers or allow management a means of checking and validating the data for exceptions (red flags) to the entered fields.

These exception reports could have triggered a review if dollar amounts or other key fields were inconsistent with chosen thresholds.

In the absence of a comprehensive set of exception reports, management lacks an efficient means of evaluating the accuracy and integrity of data modification. These exception reports could provide an extra measure of assurance that the dollar amounts are accurate. Additionally, they may provide assurance that data has not been altered inappropriately as the reports would identify altered information such as the user ID, date and time stamp, and reason for the change. These reports could provide an alert to the potential for fraud, errors, and omissions. This would provide a snapshot view of the triggers for management's review to allow for prioritized examination of key data.

**Recommendation:** We recommend that RAA work with the vendor to research and attempt to obtain additional exception reports which would be generated to identify monetary and other key triggers for review. In mitigating the risk of unauthorized/fraudulent actions, systematic reviews and approval by management should be provided. The reports should identify transaction information for review based on management thresholds. Supervisory review of

exception reports should be documented in a manner that provides evidence and support for actions taken. Potential exception reports should be documented and have management approval on a regular basis. If there are no exceptions for any given report, the report should still be generated with the date and time stamp and include a notation indicating no exceptions found.

Should the acquisition of reports be cost prohibitive, RAA should take steps to implement other manual controls, oversight, and process review steps.

**Management Response:** In current discussions with the vendor, there appear to be opportunities to acquire new exception reports at favorable pricing. RAA will pursue negotiations with the vendor in consideration of budget constraints.

## 7. **Medical Re-evaluations for Disability Retirement**

For disability retirements, counselors did not receive an automatic prompt by the system when a re-evaluation was due and were not able to determine when the members were due to be re-evaluated. This could lead to funds unnecessarily being disbursed by the county due to paying members who were able to return to work, but were not evaluated.

The PensionGold application does not keep an accurate record of all medical re-evaluation dates for members on disability retirement. The system only accepts the furthest date in the future; it does not accept all the dates entered for medical re-evaluations. When a counselor enters more than one date for the re-evaluation of disabled employees, the system ignores the dates closest to the current date and only registers the date that is farthest in the future. There are over seven hundred disabled employees currently in the PensionGold system. Of those, 468 are county employees, the remaining are the schools' employees; though, we did not include the schools' employees in our audit, it is still necessary that the system track them. The application system was designed to accept as many as ten future dates for an employee's disability re-evaluation so that a counselor could run reports of the number of re-evaluations in a particular calendar year. Section 3 -Technical Approach of the RFP states that the vendor should provide disability information such as the tracking of medical examination appointments. However, this information was not cumulatively maintained in the PensionGold database.

**Recommendation:** We recommend RAA management request that the vendor (LRS) provide a cumulative database capability of re-evaluation dates for disabled employees as stipulated by the contract. If this is not financially feasible, there should be a systematic way of ensuring that staff has reviewed the listings to accomplish the necessary re-evaluations.

**Management Response:** This is one of the agency's top priorities. The agency has created an automated spreadsheet that is used for that purpose, and negotiations are ongoing with the vendor to add this capability to PensionGold.

## 8. Editing Notes

When a counselor edited a note (comment) relating to a particular transaction or situation in the automated employee file, there was no audit trail of events, thereby erasing previous history. Rather than maintaining each edit record, the system performed a complete update and replacement. A complete history of edited notes maintained within the system provides a cumulative record of notes written as well as the date and time stamp and who entered the note. This is a records management issue in the vendor application of replacing records rather than keeping a history of all edit notes. There were no backup records to substantiate inquiries into changes made to employees' files. The lack of cumulative edit notes results in an efficiency issue for RAA staff. The lack of a note "history" limits the ability of the staff to maintain a comprehensive record of issues and actions.

**Recommendation:** We recommend that RAA request that the vendor modify the PensionGold system to cumulatively maintain edit notes.

**Management Response:** The agency is negotiating with representatives of PensionGold to address this issue. In the meantime, records of changes and change requests are being imaged and are connected to a member's file through the Laser Fiche application.