



A Report  
to the  
Board of  
Supervisors

*Maricopa County  
Internal Audit  
Department*

**Ross L. Tate**  
County Auditor

Information Technology Audit

# Human Resources Application Review

*Audit of Maricopa County's  
Human Resource Management  
Application (PeopleSoft)*

December ■ 2005

Executive Summary .....	1
Introduction .....	2
Detailed Information .....	6
Department Response .....	14

The **County Auditor** is appointed by the Board of Supervisors. The mission of the Internal Audit Department is to provide objective, accurate and meaningful information about County operations so the Board of Supervisors can make informed decisions to better serve County citizens.

## Audit Team Members

**Keri Dawson, KPMG LLP**  
**Paul Smedegaard, KPMG LLP**  
**Cheri Johnson, KPMG LLP**  
**Tammy Cox, KPMG LLP**  
**Susan Adams, Senior IT Auditor**

Copies of the Internal Auditor's reports are available by request.  
Please contact us at:

**Maricopa County Internal Audit**  
**301 W. Jefferson, Suite 1090 ♦ Phoenix, AZ 85003 ♦ (602) 506-1585**

Many of our reports can be found in electronic format at:  
[www.maricopa.gov/internal\\_audit](http://www.maricopa.gov/internal_audit)



# Maricopa County

Internal Audit Department

301 West Jefferson St  
Suite 1090  
Phx, AZ 85003-2143  
Phone: 602-506-1585  
Fax: 602-506-8957  
www.maricopa.gov

December 15, 2005

Max W. Wilson, Chairman, Board of Supervisors  
Fulton Brock, Supervisor, District I  
Don Stapley, Supervisor, District II  
Andrew Kunasek, Supervisor, District III  
Mary Rose Wilcox, Supervisor, District V

We have completed our FY 2005-06 review of the County's Human Resource Management System (PeopleSoft). This audit was performed in accordance with the annual audit plan approved by the Board of Supervisors.

The highlights of this report include:

- Access to sensitive IT administrative and end-user functionality in the PeopleSoft system is not appropriately restricted to authorized users
- User authentication to the PeopleSoft program is inconsistent and may result in unauthorized access
- Controls over PeopleSoft implementation appear adequate with no significant exceptions or control weaknesses

This report contains the executive summary, detailed findings and recommendations, and management's responses to our recommendations. We have reviewed this information with the Chief Information Officer and the Human Resources Director and appreciate the excellent cooperation provided by both departments. If you have any questions, or wish to discuss the information presented in this report, please contact Susan Adams at 506-1587.

Sincerely,

A handwritten signature in cursive script that reads "Ross L. Tate".

Ross L. Tate  
County Auditor

(Blank Page)

# Table of Contents

<b>Executive Summary . . . . .</b>	<b>1</b>
<b>Introduction . . . . .</b>	<b>2</b>
<b>Department Accomplishments . . . . .</b>	<b>4</b>
<b>Detailed Information . . . . .</b>	<b>6</b>
<b>Department Responses . . . . .</b>	<b>14</b>

# Executive Summary

## **User Access (Page 6)**

Access to sensitive IT administrative and end-user functionality in the PeopleSoft system is not appropriately restricted to authorized users. Additionally, terminated employee access is not being removed in a timely manner. Unauthorized or inappropriate access could lead to the processing of unauthorized transactions, resulting in diminished data reliability and increased risk of inappropriate data disclosure or destruction. The Human Resource (HR) Department and the Office of the Chief Information Officer (OCIO) should perform a thorough review of user access rights within the PeopleSoft program and identify and remove all user access that is not required for users' day-to-day job responsibilities.

## **User Authentication (Page 9)**

User authentication to the PeopleSoft program is inconsistent. As a result of the inconsistencies, PeopleSoft user lock-out functionality cannot be enforced and may result in unauthorized access to the PeopleSoft program. The OCIO should consider requiring all departments to use Active Directory to authenticate their users to the PeopleSoft program and develop County-wide standards for Active Directory password parameters.

## **Data Integrity and Program Interfaces (Page 10)**

No significant exceptions or control weaknesses were noted when reviewing PeopleSoft implementation controls over data record accuracy, interface design, and interface monitoring.

## **Physical Security Controls (Page 11)**

Physical security control weaknesses exist related to the PeopleSoft server room and backup tapes. Furthermore, a formal disaster recovery plan for the PeopleSoft program has not been developed. Proper physical security controls are necessary to ensure the continuity of critical application processing and data processing services, and to minimize the economic impact of an extended disruption to the PeopleSoft application in the event of a disaster. Physical security control weaknesses should be strengthened and a disaster recovery plan should be developed.

## **Policies and Procedures (Page 13)**

PeopleSoft-related policies and procedures need to be developed or expanded. Lack of complete policies and procedures could result in unauthorized program access or improper processing of human resources information. County management should develop, update, and communicate currently lacking policies and procedures.

# Introduction

## Background

In October 2002, the Board of Supervisors approved procurement of a new Human Resource Management System. The project to replace the old system was called “EAGLE,” and the vision was “to implement an integrated HR System with reengineered business processes to leverage web-based technology and electronic workflow that will maximize human capital management by Maricopa County by July 2004.”

The County chose the PeopleSoft application as its human resource system and partnered with CIBER, a third-party integrator, for the PeopleSoft implementation project. The County’s Human Resource Department (HR) is the primary owner of the PeopleSoft human resource program. PeopleSoft is run on a Hewlett Packard hardware platform on servers maintained by the Office of the Chief Information Officer (OCIO).

As of July 2005, all phases of the project have been completed, and the new PeopleSoft HR system is in production. The following table outlines the two phases of implementation and the modules that were implemented during each phase.

<b>Phase One</b> – Completed December 2003	<ul style="list-style-type: none"><li>• Human Resource (HR) Administration</li><li>• Payroll Functions</li><li>• Benefits Administration</li><li>• Time &amp; Labor</li></ul>
<b>Phase Two</b> – Primarily completed November 2004 (two modules completed in early 2005)	<ul style="list-style-type: none"><li>• Workforce Analytic – Data Warehouse</li><li>• Workforce Analytic – Scorecard</li><li>• Employee and Manager Self-Service</li><li>• Imaging</li><li>• e-Applications: e-Pay, e-Benefits, e-Performance, e-Compensation, e-Recruitment, and e-Recruitment Manager</li></ul>

The Planning and Rewards components of Workforce Analytic have not been implemented. The County is currently in the process of determining whether to implement these two modules.

## Scope and Methodology

The objective of this audit was to review the PeopleSoft Program and evaluate controls related to:

- Business Processes
- Security Management
- IT Operations
- Data Quality and Integrity

Project management controls have been specifically excluded from the scope of this audit since prior audits concluded that such controls were adequate.

This audit was performed in accordance with generally accepted government auditing standards.

# Department Reported Accomplishments

**The Office of the Chief Information Officer (OCIO) has provided the following information for inclusion in this report.**

OCIO identified the need for the re-organization of its staff and supplemental vendor support for the PeopleSoft environment. Planning, completed at the inception of the Eagle PeopleSoft project, did not account for the appropriate staff support necessary for such a system. Over the past year, OCIO has been re-organizing to align staff functions and improve system support. The newly funded senior programmer position has been difficult to fill due to the position requirements and salary range. Until the position is filled, contracted support is being utilized. Another area of concern is the System Administration support of the PeopleSoft program 24 X 7. OCIO does not have qualified PeopleSoft System Administration support. An RFP for PeopleSoft System Administration support was solicited. It includes full alarm monitoring and troubleshooting efforts.

The PeopleSoft system architecture as originally installed was not configured properly. OCIO identified the deficiencies in the hardware/software system and corrected them. New hardware was added at PeopleSoft's recommendation which improved the performance for the end users. PeopleSoft performance consultants have been contracted to assist with system tuning, which has proven beneficial. Specific to Payroll, options have been investigated to identify whether the Payroll database could be segregated from the human resource database. This is not an option for the PeopleSoft environment due to its design.

Continued improvement of the PeopleSoft experience remains the top priority of the technical support team. In addition to the above mentioned initiatives, review of business processes are also being considered to achieve efficiencies within the HR functional areas, specifically payroll processing.

As the initial Eagle project came to a close, the OCIO assembled a team of functional team leads, business managers and technical support staff to address the strategic direction of the PeopleSoft program. This team was established to look into process and program improvement. One recent initiative identified was the need to automate the Personnel Action Form (PAF) process. A team is currently working on requirements gathering to bring this tremendous opportunity to fruition. The anticipated result will be a decrease in processing time and should eliminate PAF's being submitted with incorrect data (approximately 90% of the PAF's submitted today are incorrect).

Benefits enrollment was automated, which eliminated manual entry of data allowing for reduced data entry errors and staff time savings. This year, annual Open Enrollment is now being performed directly in PeopleSoft with no paper forms being permitted also reducing errors and saving time.

All employee records are being imaged and are available on-line. This has eliminated space requirements for paper records, decreased cost of off-site data storage, improved distribution of records via appropriate request controls and allows for employees to see pertinent information directly through PeopleSoft (i.e., previous performance evaluations).

PeopleSoft was setup to communicate with the County's Active Directory user authentication security system. The same user id and password information is used for both PC/LAN and PeopleSoft access. Future projects are planned to more fully integrate PeopleSoft with Active Directory, which will automatically provision and deprovision a user's Active Directory account once this person's identity information is modified in PeopleSoft. This would eliminate the need for the LAN managers to manually enter new users or remove terminated users from Active Directory. The benefit of this would be more timely access to the systems for new employees and less risk to the County.

# Department Reported Accomplishments

**The Human Resources Department (HR) has provided the following information for inclusion in this report.**

Human Resources went live with PeopleSoft 8.8 in December 2003. Since that time we have brought up a number of additional modules, including a number of e-applications that enable our employees and managers to use self-service. As an integrated, enterprise system PeopleSoft has eliminated the need for multiple data bases, reduced the amount of re-entry of the same data elements into multiple systems and allowed us to more efficiently complete a number of processes. We have eliminated massive amounts of paper and significantly reduced cycle time in different areas. Policies and rules are now enforced uniformly by the system.

All employee time is now assigned to PAS codes, which assists us in calculating performance measures for MfR. Employees are able to update routine information themselves, freeing staff for other duties. Applicants are able to see their status online. An application is instantly available for review at the time the applicant has submitted it. Jobs may be posted the same day the requisition is received rather than waiting until the following week. We are currently piloting employee time entry and employee performance evaluations using PeopleSoft. Employee Records has begun scanning all employee personnel files, which will make them available electronically.

We continue to experience problems with the system. We have not to date stabilized our Payroll process. We have experienced crashes and near crashes and have not had the expertise to correct all of the issues surrounding time and labor that relate to Payroll. Our Payroll Staff must work long hours each pay period to ensure paychecks and direct deposits continue to meet the county deadlines.

Albeit PeopleSoft is a robust system we have not fully utilized its capacity. We implemented the initial phase of PeopleSoft in a trial and error modality. We lobbied OMB for funding for a PeopleSoft programmer and were successful in receiving the funding. We have requested that this position be filled. Unfortunately, the CIO's Office has not filled this position to date. We deem this position to be critical in helping us stabilize the systems.

We are also concerned about the impact of the new servers. We are still addressing issues of speed for end users. The farm configuration places all day-to-day operations in the same configuration which may not be the optimum configuration for such a large county operation. Running the large Payroll that we do every two weeks puts a real strain on the system. We believe an optimum way of conducting business would be to place the Payroll Operations on an independent server. We have requested that this option be explored and analyzed.

We are not sure of how all of the implementation processes to date have been documented. Recordation of operational issues is important as we continue to work through new aspects of the PeopleSoft operation. We are attempting to move toward a mode of some customization in the PeopleSoft system that was initially rolled out in a vanilla fashion as a means of cost control. We have experienced the merger of Oracle with PeopleSoft and futuristic support from Oracle may be debatable. However, there are certain aspects of the system that lend themselves to customization and would bring great relief to the end users.

One of the customizations desired centers around the Personnel Action Form (PAF). We have established a task force to flow chart the PAF in an attempt to initiate a customization process. OMB is working closely with Human Resources to accomplish this arduous task. We look forward to leadership that will take up towards the 8.9 upgrade however, we realize we must stabilize current operations prior to making that leap.

# Issue 1 User Access

## Summary

Access to sensitive IT administrative and end-user functionality in the PeopleSoft system is not appropriately restricted to authorized users. Additionally, terminated employee access is not being removed in a timely manner. Unauthorized or inappropriate access could lead to the processing of unauthorized transactions, resulting in diminished data reliability and increased risk of inappropriate data disclosure or destruction. The Human Resource (HR) Department and the Office of the Chief Information Officer (OCIO) should perform a thorough review of user access rights within the PeopleSoft program and identify and remove all user access that is not required for users' day-to-day job responsibilities.

## Security Standard

The ISO/IEC 17799 International Security Standard, a comprehensive set of controls comprising best practices in information security, states that in order to maintain effective control over access to data and information services, management should require a formal user registration process and conduct periodic reviews of user access rights. The standard goes on to discuss specific leading practice standards with regard to user access review within a multi-user information system.

## IT Administrative Functionality

Access to sensitive IT administrative functionality in the PeopleSoft production system is not appropriately restricted to authorized users. The ability to modify configuration settings, program code, and the database is not limited to the appropriate functional users.

While reviewing user access levels established within the PeopleSoft program, we noted an excessive number of users with access levels that do not coincide with their job responsibilities. The table below represents the number of user IDs and associated users with the ability to perform certain functions as of July 20, 2005. It should be noted that users may be assigned one or more user IDs to perform their job functions making the total number of user IDs greater than the total number of users. Specifically, we noted the following:

Program Functionality	Description of Access	# of User IDs with Access	# of User IDs Requiring Access	# of Users
Application Designer	User can modify the database	731	8	4
Administer Security	User can modify other user access levels	3	2	2
Superuser Access	User has access to a significant portion (999 or more pages) of the PeopleSoft program	5	2	2

Program Functionality	Description of Access	# of User IDs with Access	# of User IDs Requiring Access	# of Users
PeopleSoft Administrator	User has access to the entire PeopleSoft program through bypassing traditional security access rules	8	0	0
PeopleSoft Database Access	User can directly modify the database tables using open database connections	5	5	5

It is noted that the scope of our review was limited to PeopleSoft security. In the table above, we identified 731 users who could, theoretically, modify the PeopleSoft database using the Application Designer tool. However, possible compensating controls, outside our audit scope, may help mitigate the theoretical risk. These compensating controls include: 1) users must have access to and install the actual Application Designer client application, and 2) users must have appropriate Active Directory network permissions.

We also determined that a user ID called “Integration Broker User ID” is utilized to process system jobs. This ID allows access to the entire PeopleSoft program and is based on preset user access levels included with the purchased baseline version of PeopleSoft. County Management has not analyzed the specific functionalities this ID requires and has not performed a review of the transactions made by the Integration Broker ID.

### End-User Functionality

Access to sensitive end-user functionality in the PeopleSoft production system was not appropriately restricted to authorized users. While reviewing user access levels with management, it was noted several users with access to the PeopleSoft program did not appear to have access levels that coincided with their job responsibility. Specifically, we noted the following:

Program Functionality	Description of Access	# of User IDs with Access	# of User IDs Requiring Access	# of Users
Change Pay Rates	User updates employee pay rates	6	4	4
Check Print	User sets up check printing processes and print checks	8	6	5
Employee Processing	User updates employee data	11	8	8
Hire Employees	User hires employees	30	12	11
Pay Confirm	User confirms payroll	8	6	5
Payroll Process	User processes payroll	8	6	5

## **Terminated Employees**

Terminated employee user access is not being removed from the PeopleSoft program in a timely manner. Per review of ten Maricopa County Termination/Retirement Personnel Action forms, it was noted that all ten terminated employees selected had access for three or more days after the effective date of termination.

## **County Risks**

Unauthorized or inappropriate access could lead to the processing of unauthorized transactions, resulting in diminished data reliability and increased risk of inappropriate data disclosure or destruction.

## **Recommendations**

The HR Department and the OCIO should:

- A. Perform a thorough review of user access rights within the PeopleSoft program (including IT administrative accounts) and identify and remove user access that is not required for users' day-to-day job responsibilities. Within this review it is recommended that:
  - The IT department should not be granted update access to the functional areas of the production environment
  - Functional users should not have access to the technical system components controlled by the IT department (i.e. security administrator, application designer, process scheduler)
  - Only the System Administrator should be allowed to migrate changes into production
  - Only the Database Administrators should have direct database access
- B. Strengthen controls surrounding the use of the Integration Broker User ID including removing all unnecessary access and implementing auditing functionality around sensitive processes to review improper changes made by the Integration Broker User ID.
- C. Evaluate the current process for removing terminated employee access to the PeopleSoft program to ensure efficient and timely removal of user access.

# Issue 2 User Authentication

## Summary

User authentication to the PeopleSoft program is inconsistent. As a result of the inconsistencies, PeopleSoft user lock-out functionality cannot be enforced and may result in unauthorized access to the PeopleSoft program. The OCIO should consider requiring all departments to use Active Directory to authenticate their users to the PeopleSoft program and develop County-wide standards for Active Directory password parameters.

## Security Standard

The ISO/IEC 17799 International Security Standard, a comprehensive set of controls comprising best practices in information security, states that passwords provide a means of validating a user's identity, thus providing access rights to information processing facilities or services. The standard also discusses specific leading practice standards with regard to password parameters.

## User Authentication

User authentication is the electronic process of verifying that a user should be allowed access to a system. At the County, user authentication to the PeopleSoft program is inconsistent. Some users are authenticated by logging directly into PeopleSoft and having their password validated by PeopleSoft. Other users log directly into PeopleSoft, but their password is validated by Active Directory before connecting to PeopleSoft.

Since some users are authenticated outside of PeopleSoft, the system cannot be used to enforce account lock-out after a specified number of invalid login attempts. Moreover, the County does not require that Active Directory be configured to lock out users after a specified number of invalid login attempts. Since there are 23 different local area network (LAN) managers in the County, each responsible for establishing a given department's Active Directory password requirements, there are 23 different sets of policies and procedures.

## County Risks

Given that users authenticate to the PeopleSoft system through both PeopleSoft and Active Directory, invalid attempts to access the PeopleSoft system do not result in the account being locked out. Unauthorized access to the PeopleSoft system could result in the processing of unauthorized transactions.

## Recommendation

The OCIO should:

- A. Work with County management to enforce the use of Active Directory by all departments to authenticate all users to the PeopleSoft program.
- B. Develop County-wide standards for Active Directory password parameters.

# Issue 3 Data Integrity & Program Interfaces

## Summary

No significant exceptions or control weaknesses were noted when reviewing PeopleSoft implementation controls over data record accuracy, interface design, and interface monitoring.

## Security Standard

Data migrated from the County's former human resource management system (HRMS) to PeopleSoft should be tested and reviewed to confirm data migration was complete and accurate. Additionally, interfaces with other systems should be programmed to prevent the transfer of duplicate information and to provide error reports, and should be monitored to confirm successful data processing.

## Data Integrity

Only current employee information, as of the date of migration, was converted from the HRMS system to PeopleSoft. The HRMS system is still maintained for functional user information purposes only, as no prior history was migrated.

To ensure a complete and accurate data conversion during implementation, pre-migration employee count reports were run and compared to full reports run after migration, and all errors were resolved. Furthermore, as part of the conversion process, documentation detailing the steps and processes followed were maintained for future reference.

## Program Interfaces

Interfaces between PeopleSoft and other systems had to be developed, designed, and configured for PeopleSoft. Interfaces were tested using standard change management procedures, including final sign-off from functional users. It was also noted that Benefits interfaces were designed using requirements provided by the Benefits vendors. There are currently 10 PeopleSoft import interfaces, 20 export interfaces, and 12 Benefits interfaces.

It was noted that interfaces are monitored to confirm successful data processing. Any interface errors are researched and resolved by the appropriate department. Additionally, the direct deposit interface was selected to confirm that the interface data appears to be reconciled and monitored appropriately.

## County Risks

Erroneous data migration may result in system failures or inaccurate data processing. Poor interfaces limit business efficiencies and can result in processing errors or system failures.

## Recommendation

None, for information only.

# Issue 4 Physical Security Controls

## Summary

Physical security control weaknesses exist related to the PeopleSoft server room and backup tapes. Furthermore, a formal disaster recovery plan for the PeopleSoft program has not been developed. Proper physical security controls are necessary to ensure the continuity of critical application processing and data processing services, and to minimize the economic impact of an extended disruption to the PeopleSoft application in the event of a disaster. Physical security control weaknesses should be strengthened and a disaster recovery plan should be developed.

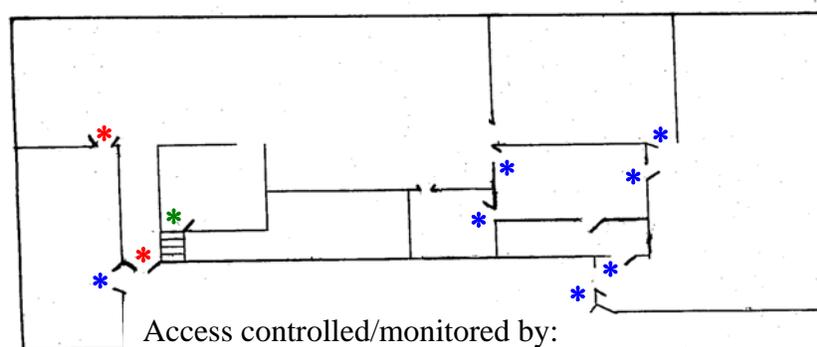
## PeopleSoft Server Room

The ISO/IEC 17799 International Security Standard, a comprehensive set of controls comprising best practices in information security, states that critical or sensitive business information processing facilities should be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage, and interference.

Protective Services, a division within the Facilities Management Department (FMD), and the County Attorney's Office (MCAO) control access to different doors that lead to a central server room where the PeopleSoft servers are located. As a result, if the MCAO grants access to the server room, they are also granting access to the PeopleSoft servers without appropriate PeopleSoft management authorization.

It was also noted that both groups have inconsistent access requirements, access review policies, and access monitoring/alarm response procedures. For instance, some door alarms are monitored 24 hours a day, seven days a week, while other door alarms are only monitored during business hours. Inconsistent access requirements and inconsistent physical security may result in unauthorized access to the server room.

## Diagram of Server Room



Access controlled/monitored by:

- \* Facilities Management
- \* County Attorney
- \* Key Access Only

In addition, one door having direct access to the server room has key access only. While controls exist over the keys and FMD maintains a log of key holders, proper monitoring and restriction of physical access is strengthened through use of an electronic card reader security system.

### **Backup Tapes**

ISO/IEC 17799 states that to maintain the integrity and availability of information processing and communication services, routine procedures should be established for carrying out the agreed backup strategies.

The daily incremental backup tapes of the PeopleSoft production environment are stored on a storage area network (SAN). The SAN server is located in the same physical location as the production server. Currently, the backup tapes are rotated off-site once a week. If a disaster were to occur and the SAN was damaged, the County could lose up to five days worth of transaction data.

### **Disaster Recovery Planning**

ISO/IEC 17799 states that to maintain the integrity and availability of information processing and communication services, routine procedures should be established for carrying out the agreed backup strategies.

A documented comprehensive PeopleSoft disaster recovery plan, clearly outlining how the County will recover in the event of an extended disruption of the PeopleSoft program, does not exist. A documented disaster recovery plan is important to ensure the continuity of critical application processing and data processing services, and to minimize the economic impact of an extended disruption to the PeopleSoft program in the event of a disaster.

### **Recommendations**

- A. FMD and MCAO, in conjunction with the OCIO, should establish a formalized policy and procedure for granting, removing, and monitoring access to the server room.
- B. FMD should install a card reader on the door currently with key access to allow for proper monitoring and restriction of physical access to the room.
- C. The OCIO should put all incremental backup tapes in a secure location (e.g., fireproof safe or temporary off-site secure location) until an alternate permanent off-site location can be identified to house the storage area network (SAN).
- D. The OCIO should develop a formal disaster recovery plan to minimize the disruption to operations in the event of a disaster or other unplanned outage of the PeopleSoft program. The plan should be periodically tested to help identify weaknesses in the plan and provide management with a more accurate assessment of the time and effort necessary to recover data processing capability.

# Issue 5 Policies & Procedures

## Summary

PeopleSoft-related policies and procedures need to be developed or expanded. Lack of complete policies and procedures could result in unauthorized program access or improper processing of human resources information. County management should develop, update, and communicate currently lacking policies and procedures.

## PeopleSoft Security Administration Policy

Formally documented security administration policies and procedures do not exist. Security Standards state that access to a multi-user information system should be controlled through a formal user registration process. The lack of documented security administration policies and procedures decreases user accountability and increases the risk that excessive levels of access rights will be assigned or retained by unauthorized users.

## User Access Request

While reviewing the process for granting access to PeopleSoft, it was noted that IT users are not required to complete the 'User Access Request' form to gain access to the application or the database. Management has started the process for developing the necessary procedures for implementing a user access request form. Unauthorized or inappropriate access within PeopleSoft could result in the processing of unauthorized transactions.

## PeopleSoft Desktop Procedures

To enhance control monitoring, desktop procedures should be created and formalized to reflect current procedures. Comprehensive desktop procedures accurately reflecting current PeopleSoft procedures have not been updated or completed in the Recruiting, Benefits, and Records areas of the HR Department. Although formal desk top procedures are not completed, the areas noted above have begun to update and create desktop procedures. Lack of formal desktop procedures could result in improper processing of human resources information.

## Recommendations

- A. The OCIO should develop, document, and communicate formal guidelines for administering PeopleSoft Security.
- B. The OCIO should continue efforts to develop an IT personnel 'User Access Request' form.
- C. The HR Department should complete and update all PeopleSoft desktop procedures.

# Department Responses





# Maricopa County

Facilities Management

401 West Jefferson Street  
Phoenix, Arizona 85003-2115  
Phone: (602) 506-1141  
Fax: (602) 506-4275  
Customer Service: (602) 506-3277

## Human Resources Application Review Facilities Management Department - November 29, 2005

### **Issue #4 Physical Security Controls:**

The ISO/IEC 17799 International Security Standard, a comprehensive set of controls comprising best practices in information security, states that critical or sensitive business information processing facilities should be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage, and interference.

Protective Services, a division within the Facilities Management Department (FMD), and the County Attorney's Office (MCAO) control access to different doors that lead to a central server room where the PeopleSoft servers are located. As a result, if the MCAO grants access to the server room, they are also granting access to the PeopleSoft servers without appropriate PeopleSoft management authorization.

It was also noted that both groups have inconsistent access requirements, access review policies, and access monitoring/alarm response procedures. For instance, some door alarms are monitored 24 hours a day, seven days a week, while other door alarms are only monitored during business hours. Inconsistent access requirements and inconsistent physical security may result in unauthorized access to the server room.

**Response:** Concur. FMD believe that all the doors should be on the County's Access Control System. We recommend that FMD convert the two card readers that are on the County Attorney's Security System and tie them into the County system. This would ensure that FMD can monitor all the doors for the entire area 24 hours per day for security breaches.

**Recommendation A:** FMD and MCAO, in conjunction with the OCIO, should establish a formalized policy and procedure for granting, removing, and monitoring access to the server room.

**Response:** Concur - will initiate discussions immediately. FMD recommends the removal of the two card readers from the County Attorney's Office system and adding these readers to the FMD managed County system, Momentum. If agreed to by the County Attorney's Office, FMD will work with both the County Attorney and the Office of the Chief Information Officer to develop policies and procedures regarding access to the server room.

Target Completion Date: 6/01/06

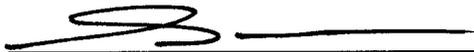
Benefits/Costs: Increased control over access, 24 hour monitoring and better accountability.

**Recommendation B:** FMD should install a card reader on the door currently with key access to allow for proper monitoring and restriction of physical access to the room.

Response: Concur - Will initiate the removal of the existing key lock and the installation of a card reader.

Target Completion Date: 2/25/06

Benefits/Costs: Improved control over access and better accountability.

Approved By :  \_\_\_\_\_ 11/30/05  
Department Head/Elected Official Date

 \_\_\_\_\_ 11-30-05  
Chief Officer Date

 \_\_\_\_\_ 12/6/05  
County Administrative Officer Date

**AUDIT RESPONSE—HUMAN RESOURCES APPLICATION REVIEW**  
**OFFICE OF THE CHIEF INFORMATION OFFICER**  
**December 8, 2005**

**Issue #1:**

**Access to sensitive IT administrative and end-user functionality in the PeopleSoft system is not appropriately restricted to authorized users. Additionally, terminated employee access is not being removed in a timely manner .**

**Response: Concur**

**Recommendation A:** Perform a thorough review of user access rights within the PeopleSoft program (including IT administrative accounts) and identify and remove user access that is not required for users' day-to-day job responsibilities. Within this review it is recommended that:

**Application Designer access: Concur – will implement with modifications.** Only users that have Application Designer installed on their workstation can access Application Designer. The 731 users with access listed are referring to a common permission list, which works hand-in-hand with the Application Designer client product. Without the client product installed on the workstation and without proper network drive permissions, no access is possible. At present only four users have access to Application Designer. The remaining accounts do not have access to this program. Action will be taken to remove this common permission list from all users that do not require access to this application.

**Administer Security access: Concur.** Auditors are referring to a Mainframe computer operator who assists the Security Access Administrator in creating and maintaining user ids. The operator does not require full security admin access to perform that function, and will have his/her user account modified to limit access to only User Profile maintenance activities.

**Superuser Access: Concur.** Super User access will be restricted. Two user id's will continue to have this level of access due to system functionality and business continuity requirements.

**PeopleSoft Administrator: Concur – will implement with modifications.** System Administrators and Security Administrators must possess the PeopleSoft Administrator role in production; otherwise their essential job duties would be severely impaired. Additional controls will be activated as required to audit changes made to critical tables.

**PeopleSoft Database Access: Concur.** No Action Required.

- The IT department should not be granted access to the functional areas of the production environment

**Response: Concur – will implement with modifications.** System Administrators and Security Administrators must possess the PeopleSoft Administrator role in production;

otherwise their essential job duties would be severely impaired. Controls will be put into place to audit changes to critical tables.

Target Completion Date: April 2006

Benefits/Costs: Increased control over system integrity and user accountability. In-house staff will complete the activities. No additional costs would be incurred.

- Functional users should not have access to the technical system components controlled by the IT department (i.e. security administrator, application designer, process scheduler).

Response: **Concur.** No Functional users have access to technical system components.

Target Completion Date: Not applicable.

Benefits/Costs: Not applicable.

- Only the System Administrator should be allowed to migrate changes into production

Response: **Concur – will implement with modifications.** Critical security administration would be curtailed if the Security Administrator does not have ability to migrate security objects into production. For example, role maintenance could be delayed for a period of up to 2 weeks, instead of the customary same or next day action. Processes to monitor and report on all migration activities will be developed and implemented as with thorough quality assurance functions.

Target Completion Date: April 2006

Benefits/Costs: Increased control over system integrity and user accountability. In-house staff will complete the activities. No additional costs would be incurred.

- Only the Database Administrators should have direct database access.

Response: **Concur - will implement with modifications.** Will ensure that only the Database Administrators have direct database access to all tables. The PeopleSoft Security Administrator must have direct access to all security tables in order to perform his duties administrating program security. Changes to these tables will be audited.

Target Completion Date: April 2006

Benefits/Costs: Increased control over system integrity and user accountability. In-house staff will complete the activities. No additional costs would be incurred.

**Recommendation B:** Strengthen controls surrounding the use of the Integration Broker User Id including removing all unnecessary access and implementing auditing functionality around sensitive processes to review improper changes made by the Integration Broker User Id.

**Response: Concur - in process.** The Integration Broker User Id is a system id, not a user id. This system id is only used by Integration Broker to authenticate transactions between individual PeopleSoft application modules and/or external systems. Implementing auditing to monitor changes made to tables will be reviewed in conjunction with the HR since activating this feature may negatively impact PeopleSoft performance. If concurrence is reached, additional controls will be activated as required to audit changes made to critical tables.

**Target Completion Date:** April 2006

**Benefits/Costs:** Increased control over system integrity and user accountability. In-house staff will complete the activities. No additional costs would be incurred.

**Recommendation C:** Evaluate the current process for removing terminated employee access to the PeopleSoft program to ensure efficient and timely removal of user access.

**Response: Concur.** At present, a nightly process is executed in PeopleSoft to lock terminated employees after the termination paperwork has been processed through HR. HR will respond to this recommendation regarding the current business process for removing terminated employee access to the PeopleSoft system.

**Target Completion Date:** HR management will respond to this under a separate submission.

**Benefits/Costs:** HR management will respond to this under a separate submission.

**Issue #2:**

**User authentication to the PeopleSoft program is inconsistent. As a result of the inconsistencies, PeopleSoft user lock-out functionality cannot be enforced and may result in unauthorized access to the PeopleSoft program.**

**Response: Concur.**

**Recommendation A: Work with County Management to enforce the use of Active Directory by all departments to authenticate all users to the PeopleSoft program.**

**Response: Concur - in process.** A workgroup has been engaged to evaluate and recommend feasible solutions for all County departments to either use a single Active Directory forest or be able to work between multiple forests. To mitigate these inconsistencies an enterprise single sign-on authentication process must be adopted and adhered to by all County departments. Current IT County policy does not appear to apply to Elected Offices and Special Districts.

**Target Completion Date: July 2007**

**Benefits/Costs: Increased control over system integrity and user accountability. Costs will be associated with any solution selected to correct this deficiency. Cost estimates will be prepared upon the review of each identified solution.**

**Recommendation B: Develop County-wide standards for Active Directory password parameters.**

**Response: Concur - in process.** This recommendation is dependant on the completion of Issue #2 - Recommendation A above.

**Target Completion Date: July 2007**

**Benefits/Costs: Increased control over system integrity and user accountability. In-house staff will complete the activities. No additional costs would be incurred.**

**Issue #3:**

**No significant exceptions or control weaknesses were noted when reviewing PeopleSoft implementation controls over data record accuracy, interface design, and interface monitoring.**

**Response: Concur.**

**Recommendation: None. For information only.**

**Issue #4:**

**Physical security control weaknesses exist related to the PeopleSoft server room and backup tapes. Furthermore, a formal disaster recovery plan for the PeopleSoft program has not been developed.**

**Response: Concur.**

**Recommendation A:** FMD and MCAO, in conjunction with the OCIO, should establish a formalized policy and procedure for granting, removing, and monitoring access to the server room.

**Response: Concur - in process.**

The OCIO in conjunction with FMD, MCAO, MCSO, Assessor, ICJIS and Schools will convene a workgroup to address this matter. These are the departments that have IT resources housed in the referenced server room. This group will work through the process of formalizing procedures for granting, removing and monitoring access to the sever room in compliance with County policies, standards, guidelines and procedures.

**Target Completion Date: July 2006**

**Benefits/Costs:** Increased control over system and data integrity. In-house staff will complete the activities. Costs will be determined upon final recommendation of this working group.

**Recommendation B:** FMD should install a card reader on the door currently with key access to allow for proper monitoring and restriction of physical access to the room. In the interim, FMD should replace the lock and create a log of all keys issued.

**Response: Concur - in process.** The OCIO will work with FMD to install a card reader on the keyed access door and in the interim ensure control over all keys issued for door access to the server room.

**Target Completion Date: July 2006**

**Benefits/Costs:** Increased control over system integrity and user accountability. Cost will be incurred to purchase, install and configure the card reader.

**Recommendation C:** The OCIO should put all backup tapes in a secure location (e.g., fireproof safe or temporary off-site secure location) until an alternative permanent off-site location can be identified to house the storage area network (SAN).

**Response: Concur- will implement with modifications.** At present backup tapes are created and sent to a secure offsite location on a weekly basis. Additionally we are evaluating time/effort/cost associated with performing daily tape backups. A feasibility study is also being performed to identify an alternate permanent offsite location to house the SAN and/or a secondary mirrored SAN (which includes the migration plan to establish a master storage solution).

**Target Completion Date: July 2006**

**Benefits/Costs:** Increased control over system and data integrity. Costs will be associated with any solution selected to correct this deficiency. Cost estimates will be prepared upon the review of each identified solution.

**Recommendation D:** The OCIO should develop a formal disaster recovery plan to minimize the disruption to operations in the event of a disaster or other unplanned outage of the PeopleSoft program. The plan should be periodically tested to help identify weaknesses in the plan and provide management with a more accurate assessment of the time and effort necessary to recover data processing capability.

**Response:** **Concur - in process.** The procurement process will begin for technical assessments and evaluations for disaster recovery. The vendor selection and work commencement is estimated to occur no later than January 30, 2006. Achieving this date is contingent upon the available base of Materials Management vendor contracts and/or RFP process timelines.

**Target Completion Date:** June 2007

**Benefits/Costs:** Increased control over system and data integrity. Costs will be associated with the selection of a third party vendor to complete the disaster recovery evaluation. Further costs will be associated with implementation of the vendor's recommendations.



## **Audit Reponses from Central Human Resources**

### **Issue 1 User Access**

#### **Summary**

Access to sensitive IT administrative and end-user functionality in the PeopleSoft system is not appropriately restricted to authorized users. Additionally, terminated employee access is not being removed in a timely manner. Unauthorized or inappropriate access could lead to the processing of unauthorized transactions, resulting in diminished data reliability and increased risk of inappropriate data disclosure or destruction. The Human Resource (HR) Department and the Office of the Chief Information Officer (OCIO) should perform a thorough review of user access rights within the PeopleSoft program and identify and remove all user access that is not required for users' day-to-day job responsibilities.

#### **Recommendation**

The HR Department and the OCIO should:

- A. Perform a thorough review of user access rights within the PeopleSoft program (including IT administrative accounts) and identify and remove user access that is not required for users' day-to-day job responsibilities. Within this review it is recommended that:
  - The IT department should not be granted access to the functional areas of the production environment
  - Functional users should not have access to menus allowing configuration changes
  - Only the System Administrator should be allowed to migrate changes into production
  - Only the Database Administrators should have direct database access

#### **Response**

The purpose of implementing PeopleSoft was to develop an integrated, decentralized system for end users across the 59 agencies of Maricopa County. Albeit we agree with your recommendation that the IT department should not be granted access to the functional areas of the production environment, we must respectfully disagree with the second specified bullet point.

Functional users must have the ability to configure changes in order to conduct human resources business. A palpable example of that need is seen in the E-Recruit PeopleSoft module. Posted positions require supplemental questionnaires and these vary according to

position requirements. Staffing continually reconfigures on a daily basis to meet the needs of our customers.

Benefits is another important area where reconfiguration takes place during open enrollment and when policy changes dictate a need.

Likewise Payroll must reconfigure to establish new earning codes. Policy changes such as severance require changes in earning codes. Additionally, both Payroll and Records are responsible for tax updates necessitating reconfiguration. We disagree with the numbers for end users listed in your charts and would like to work with you defining who the actual end users are for the specific functional areas you have listed.

The remaining two bullet points make sense to us and we are in agreement.

### **Target Completion Date**

We do not agree to changes in functional user configuration and are not recommending a change in that practice. We do agree with eliminating IT's access to the functional environment of production, permitting the System Administrator to migrate changes into production and permitting the Database Administrator only to access the database. These changes can be implemented effective December 1, 2005.

### **Benefits/Costs**

We are unaware of any associated costs with the implementation of the procedures.

- B. Strengthen controls surrounding the use of the Integration Broker User Id including removing all unnecessary access and implementing auditing functionality around sensitive processes to review improper changes made by the Integration Broker User Id.

### **Response**

This is an IT issue that should be addressed through the CIO's Office.

- C. Evaluate the current process for removing terminated employee access to the PeopleSoft program to ensure efficient and timely removal of user access.

### **Response**

Employees are terminated after a termination PAF that typically is generated to Records. The entry of the termination into PeopleSoft generates a notice to OCIO Security that locks out the user within 24 hours. The problem identified lies not with the process of Central HR terminating employees in the system. The problem is one of a long-standing business practice where decentralized departments do not generate PAF's in a timely

manner to Records nor do they call the IT department to remove access of the terminating employee. We agree that this business practice needs to change. We have Kirk Jaeger investigating workflow in terms of the PAF to re-engineer and create a more efficient process. This is a process improvement that we hope to have implemented prior to fiscal year 2007.

**Target Completion Date**

May of 2006

**Benefits/Costs**

We do not envision any additional costs associated with the re-engineering of the PAF process

**Issue 5 Policies & Procedures**

**Summary**

PeopleSoft-related policies and procedures need to be developed or expanded. Lack of complete policies and procedures could result in unauthorized program access or improper processing of human resources information. County management should develop, update, and communicate currently lacking policies and procedures.

**Recommendation**

The HR Department should complete and update all PeopleSoft desktop procedures.

**Response**

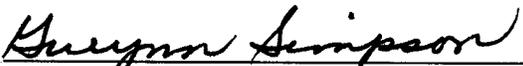
Payroll/Records have completed their desktop procedures. Staffing and Recruiting are in the process of updating these and we agree with you on this important issue. Benefits is not a part of HR and we are unsure as to progress made on updating their desktop procedures.

**Target Completion**

June, 2006



David Smith – County Manager



Gwynn Simpson – Human Resources Director