

**PEOPLESOFT AUDIT
AUDIT ITS 06-01
OCTOBER 26, 2006**



CITY OF TAMPA

Pam Iorio, Mayor

Internal Audit Department

Roger Strout, Internal Audit Director

October 26, 2006

Honorable Pam Iorio
Mayor, City of Tampa
1 City Hall Plaza
Tampa, Florida

RE: PeopleSoft Audit, Audit ITS 06-01

Dear Mayor Iorio:

Attached is the Internal Audit Department's report on PeopleSoft.

We thank the management and staff of Technology & Innovation (T&I), Human Resources, and Payroll for their cooperation and assistance during this audit.

Sincerely,

Roger Strout
Internal Audit Director

cc: Darrell Smith, Chief of Staff
James Buckner, Director of Technology and Innovation
Bonnie Wise, Director of Revenue and Finance
Kimberly Crum, Director of Human Resources
Lee Huffstutler, Chief Accountant

**PEOPLESOFT AUDIT
AUDIT ITS 06-01
OCTOBER 26, 2006**

Charlene Kiyawa
Auditor

Y. St
Audit Supervisor

Roger Strait
Audit Director

PEOPLESOFT AUDIT AUDIT ITS 06-01

INTRODUCTION

The PeopleSoft Human Resource Management System (HRMS) is a web-based application that supports the City of Tampa's Human Resources needs. Specifically, HRMS assists with administrating the workforce, managing positions, planning salaries, meeting regulatory reporting requirements, maintaining employee benefits, maintaining employee payroll deductions, and processing payroll.

This is the first audit of PeopleSoft.

STATEMENT OF OBJECTIVES

This audit was conducted in accordance with the Internal Audit Department's FY06 Audit Agenda. The objectives of this audit were to determine that:

1. The policies and procedures for administrating access to PeopleSoft were adequate.
2. Access to critical PeopleSoft application transactions were adequately restricted and were properly segregated.
3. PeopleSoft Application Functions and PeopleTools were restricted to personnel who require access to them and those personnel had the appropriate permissions to use the application.

STATEMENT OF SCOPE

The audit testing emphasized current status as of the 3rd and 4th quarter of fiscal year 2006. Source documentation was obtained from the Technology and Innovation Department (T&I). Original records as well as copies were used as evidence and verified through physical examination.

STATEMENT OF METHODOLOGY

Computer processed data was not used to arrive at our conclusions; therefore, we are not required to assess or attest to the reliability of this type of data.

The configuration of the data did not lend itself to statistical sampling. Additionally, since we did not intend to infer the sample results to an overall population, judgmental samples were used in some areas of our test work. This improved the overall efficiency of the data selection and analysis.

STATEMENT OF AUDITING STANDARDS

We conducted our audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to afford a reasonable basis for our judgments and conclusions regarding the organization, program, activity or function under audit. An audit also includes assessments of applicable internal controls and compliance with requirements of laws and regulations when necessary to satisfy the audit objectives. We believe that our audit provides a reasonable basis for our conclusions.

AUDIT CONCLUSIONS

Based upon the test work performed and the audit findings noted below, we conclude that:

1. Procedures for administrating PeopleSoft access were generally adequate. However, terminated, retired, or deceased employee's PeopleSoft User IDs were not deleted in a timely manner.
2. Access to the PeopleSoft application (i.e. personnel changes, pay rate changes, etc) was granted to individuals that did not require the rights.
3. Access to the PeopleSoft Application Functions and PeopleTools (i.e. Security Administration, Application Designer, etc.) were not restricted to authorized personnel.

While the findings discussed below may not, individually or in the aggregate, significantly impair the PeopleSoft application, they do present risks that can be more effectively controlled.

T&I ACCESS TO PRODUCTION DATA

Adequate controls for the segregation of duties in the production environment and the data production functions are essential to provide assurance of the reliability of the data. Application developers should not be granted access to production data. Our tests of access permissions found that Technology and Innovation application developers had permissions to update PeopleSoft production data. During the implementation of PeopleSoft, beginning in 2002, application developers assisted the business users who were new to the program in monitoring and troubleshooting the application. We determined that T&I staff could still provide this support when it is needed; however, access to production is not required for them to support the business users.

RECOMMENDATION 1

Access to production PeopleSoft data for T&I application developers should be removed.

AUDITEE RESPONSE

Agree with a minor exception. Under the current software development environment, access to the production system is required by the on-call group comprised of the T&I Lead Analyst, two Sr. Application Programmer Analysts, and a Technical Support Analyst. Their responsibilities are to be available to troubleshoot application issues that arise during daily processing and provide quick turnaround for incidents during critical events, such as the weekly payroll cycle. To ensure the on-call staff is able to thoroughly understand the incident, access to *view* production information is often required for accurate response. In the future, we hope to have a system architecture enabling all software engineers to not require access to any production systems.

Auditee Comment: We recommend that until the proper environment is established, the T&I PeopleSoft (PS) on-call staff be granted inquiry-only access to production PS data. This will be accomplished through the creation of a new PS on-call role comprised of the cloning of the current COT Permission Lists into CT[permission list name], setting the permission to display only, and assigning the PS on-call user accounts to the role.

ACCESS CONTROLS

Application security access provides reasonable assurance that data is protected against unauthorized use, modification, disclosure, loss, or impairment. Inadequate access controls diminish the reliability of computer processed data. The purpose of controlling access to data and information is to ensure (1) users have only access needed to perform their duties, (2) access to sensitive resources is limited to only those for which it is required to carryout their job functions, and (3) employees are restricted from performing incompatible functions or functions beyond their job responsibilities. Our test work disclosed that a few individuals were granted access to human resource and/or payroll functions that exceeded their level of job responsibility.

RECOMMENDATION 2

The access granted to individuals that is incompatible with the level of their duties should be removed. A periodic review of the access levels within PeopleSoft should be performed and documented to ensure that the access granted is still appropriate.

AUDITEE RESPONSE

Agree. The individuals referred to in the recommendation are end-users who have some update access to production data. The extent of the access is in the process of being limited to only the authority consistent with their business functions. The changes are made by updating their roles and permissions based on information received from HR/Employee Relations.

To ensure consistency, a quarterly report will be generated by T&I showing access levels within PeopleSoft. The list will be approved by HR.

ACCESS TO PEOPLETOOLS

PeopleTools provides the underlying technology for the PeopleSoft application. The application is built, deployed, and maintained using PeopleTools. It encompasses tools for development, security administration, upgrades, reporting and analysis, and integration. Proper segregation and assignment of access to PeopleTools is essential in providing assurance of the reliability of the data. Our test work disclosed instances when access was not appropriate. We found T&I application developers with access to PeopleTools that could migrate modules from the Quality Assurance environment to production. Other individuals, who do not perform Security Administrator job responsibilities, had access to security administrator functions.

RECOMMENDATION 3

The incompatible access should be corrected. A periodic review of access granted to PeopleTools should be incorporated into the review recommended in recommendation 2.

AUDITEE RESPONSE

Agree with exceptions. Under the current software development environment, specific, non-standard accesses are required to perform software migration from development, to test, then to production.

The PeopleSoft application migration schema is currently set up in a non-standard methodology to authorize specific individuals' migration authority from development (DEV) to test (QA) environments. Migration to production (PRD) is granted to the T&I Database Admin (DBA) group only. To ensure that the DBA group only has authority to perform permitted project migrations, and does not have access to page information, the COT Migration role will be used by authorized DBA staff. Further, the roles assigned to the DBA user group will be modified to eliminate all roles not required for the group's job duties.

Roles to be removed from DBA User ID group:

- COT Audit QRY User
- COT Custom Menus Pages
- COT HR Administrator
- COT HRMS Administrator
- COT PT Migration Mngr
- COT Payroll Admin
- COT Query User
- COT Report Super User
- COT Report User
- COT ReportDistAdmin

PeopleSoft Administration
PeopleTools
Query Designer
Query User

Under the current software development environment, the PS developer group requires access to PeopleTools capability in the QA environment for troubleshooting duties. The appropriate role for their job assignments is titled the “PS Support” role. This role will not include Security Administration permission.

The individuals authorized to migrate projects within the Support environment will be assigned to a new role, titled “PS Admin,” which will include Security Administration permission for Support environments. To ensure these roles are properly created, the DBA will enable the roles in QA after the weekly refresh from PRD, where the roles are disabled.

The Security Administration role will be granted to only the standard ‘PS’ User IDs as required by PeopleSoft for software upgrades and to the T&I Security Office individuals authorized to maintain PeopleSoft production security.

To ensure consistency, a quarterly report will be generated and reviewed by T&I showing access levels for each person.

Auditee Comment: We recommend that until the proper environment is established, the non-standard methodology described above for permissions be granted.

REMOVAL OF USER ID'S FOR TERMINATED, RETIRED, AND DECEASED EMPLOYEES

In computer applications, user security defines the specific functions an individual user can perform and what data they can access. Security Administrators have the responsibility for establishing a new user's access, revising access when an individual transfers to another department and, deleting access when the individual leaves the City. Our test work disclosed several active PeopleSoft User IDs assigned to terminated, retired, and deceased employees. The City utilizes Novell Directory Services (NDS) for many of its applications. Users log onto the network and NDS determines their access rights. NDS supports LDAP (Lightweight Directory Access Protocol) as the protocol that allows a user to have a single sign-on for multiple applications (i.e. PeopleSoft, GroupWise, Internet, etc). We found that the associated LDAP access for the PeopleSoft User IDs noted above was disabled or deleted. This prevents a user with an active PeopleSoft user ID from signing on to the system. Although there is little risk, it is a good business practice to delete application access for terminated, retired, or deceased individuals in a timely manner.

RECOMMENDATION 4

T&I should remove all active PeopleSoft User ID's for terminated, retired, and deceased employees. In addition, the current procedures for removing access to the network, operating systems, and the applications should be reviewed to ensure that all access is removed in a timely manner.

AUDITEE RESPONSE

Agree. Internal Audit provided T&I Security Office a list of User ID's targeted for removal from PeopleSoft security roles. The process to remove these users has been completed. As the employees assigned to these User ID's are no longer active, their network logins are inactive and they would not be able to gain access to the PeopleSoft system, regardless of the presence of assigned roles in the application.

To ensure continued consistency, a quarterly report will be generated and reviewed by T&I.