2009-A22

Metropolitan Council

Program Evaluation and Audit

PeopleSoft Financial System Review

March 18, 2009

INTRODUCTION

Background

This report presents a review of the PeopleSoft Financial System (PFS), which is the Metropolitan Council's official enterprise financial system. The PFS was originally implemented in 1997 and the most recent upgrade was in 2006. Given the importance of the PFS to the financial management of Council resources, the system is considered high risk and was added to the audit work plan for 2008.

Purpose

The purpose of the PFS review was to identify potential risks and weakness in controls as well as identify solutions to mitigate risks and strengthen controls. This review is also intended to determine that controls ensure the accuracy and completeness of data processed in the system and that output is accurate and distributed to authorized personnel in a timely basis.

Scope

This audit included a review of user roles and responsibilities, system security, system inputs and outputs, system recovery, and a user survey. The review was limited to PFS Production environment. The test and development environments were not reviewed.

Methodology

Data Collection

Interviews were conducted with:

- IS staff
- Finance department staff
- System users
- Staff associated with interfaced systems

The following information was reviewed:

- Contracts with Oracle
- System access control and security
- System support
- Map of system inputs and outputs
- Data flow

Surveys

- Internal system users were surveyed about their experiences with the system
- Other governmental units were surveyed on staffing levels to support financial systems

Evaluation

The following system elements were evaluated for the presence of adequate controls:

- Password integrity
- User rights
- System security
- The ability to recover from unexpected shutdowns while maintaining data integrity.

Assurances

This review was conducted in conformance with *Government Auditing Standards* and the *Standards for the Professional Practice of Internal Auditing* of the Institute of Internal Auditors.

OBSERVATIONS

PeopleSoft Financial System (PFS) User Feedback

Audit conducted a survey of 248 Council employees who have access to PFS. A total of 99 employees participated in the survey representing a 40% response rate. Four of the surveys were deemed “incomplete” because they lacked sufficient responses bringing the final response rate to 38%. An additional seven employees responded by email that they never use the system. A copy of the survey and the aggregate survey results are provided in Appendix A.

The survey participants were asked to identify the area of the Council in which they worked. The largest percentage of respondents, 43%, were from Regional Administration. Metro Transit represented 35% of the respondents while the remainder were from Environmental Services.

Survey participants were asked to identify which division of the Council they were in, how frequently they used PFS, what training they have had, who trained them and which modules of the PFS System they use.

Most PFS users are not accessing the system.

Audit found that 58% of the identified system users have not accessed the system in more than a year. Audit also found that 43% have *never* accessed the system although they have been identified as users.

There is a need for additional training.

Fifty three percent of the respondents reported they had received PFS training. Training varied across PFS users depending on their system needs, such as those who enter transactions and create reports versus users who only review reports. PFS respondents who only review reports on the system were most likely to have received no training. Most survey respondents who enter transactions or create reports in the PFS reported receiving training. Of survey respondents who enter transactions in PFS, 79% reported receiving training. Also, 74% of respondents who create reports said that they received some training. Only 41% of respondents who only review reports reported having received training.

The survey showed that trained individuals use the PFS more frequently (i.e. daily or weekly) and are generally more satisfied with its functionality. They also utilize more modules and features.

Based on the number of respondents who haven’t had any training and those who have been trained but would like more training there is a need for additional training. In Regional Administration and Metro Transit, employees on average would like training on either one or two modules. In Environmental Services however, only two of the respondents indicated that they would like to receive any additional or refresher training.

Survey respondents cited Reporting Tools and Query Builder most often as the modules for which additional training is desired.

It is a prudent business practice to ensure that employees who use the PFS are properly trained on its capabilities and functionality. Proper training on the capabilities of the PFS will result in better utilization of the system and, in turn, increased productivity.

Most PFS users receive assistance from PFS support staff most often, and users indicate that they are satisfied with the help they receive from support staff.

PFS support staff consists of two Business System Analysts based at the Robert Street offices. The PFS support staff are also the PFS administrators. PFS users indicated that they get help from PFS support staff or people in their own department most often; 38% of respondents indicated getting assistance from PFS support staff most often and 35% indicated getting help from other employees in their department most often. The survey indicated that 77% of respondents said they were satisfied or very satisfied with assistance from PFS support staff.

At the same time, some comments on the survey found that a few users were not aware that PFS support staff was available for assistance. The Council Intranet Site has a PeopleSoft Financial System link which does list who to call for help but comments to Audit revealed that some users are unaware of this resource.

At Metro Transit, most users seek help from staff within their own department. During the audit, one of the two PFS support staff spent a week at Metro Transit. Metro Transit staff reported that this was very helpful. MT staff reported that they were able to demonstrate the issues that they were experiencing and, in turn, found that there may be solutions in place to address these issues.

Since such a large portion of users are untrained themselves (47%), there is a risk that assistance from within their own department may come from someone who does not fully understand the PFS. The potential exists for the use of incorrect or inefficient procedures to become the standard process for individual departments when there isn’t communication between the users and the PFS support staff.

System Controls

Security administration functions control the access to the applications and data stored within PFS and support the confidentiality and integrity of the data. PFS access is defined by the assignment of user IDs to various roles within PFS. Within the roles the user has permission lists and menu items that are assigned to them with varying levels of access. Audit reviewed a list of all user IDs and the roles, permission lists and subsequent menu items assigned to them. This list was then reviewed with various functional personnel to determine the appropriateness of the roles, permission lists and menu items assigned to the user IDs. Audit also analyzed the different access provided to users who were in similar jobs or had high level access rights within the system. Particular attention was paid to appropriate segregation of duties.

Audit identified some limited but significant control weaknesses in the security of group login IDs.

Most PFS users are granted access to the system with an individual login ID, and the access rights attached to that login ID should be appropriate to the individual's position as determined by their manager and the PFS administrator. Audit identified seven login IDs for the PFS that are not for individual people but for groups who access the system for specific, limited purposes. Generally, these group login IDs have higher level access rights assigned to them. Given the inherent risk associated with these types of login IDs, Audit checked on all such IDs as to their purpose and found that five of the seven group login IDs present a potential security risk to the PFS.

a. A limited number of login IDs with higher-level access rights could not be accounted for.

Audit found that two login IDs are of unknown purpose. PFS administrators indicated that the one login may have been used by an IS staffer at one time. However, the login has not been used since spring of 2008 and the access rights associated with that login are greater than the access rights granted to the associated IS staff person. The PFS administrators have also presented other ideas to Audit on the purpose of this login ID.

The second login has high level security access assigned to it, but PFS administrators have conflicting recollections as to the purpose of this login ID. PFS administrators could not provide any documentation showing the purpose of either login ID.

b. Three group login IDs created for a temporary purpose were never deactivated from the PFS.

Audit found three generic login IDs that had been created for the last PFS upgrade in 2006. While these login IDs were created for a temporary purpose, they were never locked from the system after the upgrade was complete. One of these login IDs had the highest level of access rights assigned to it. It had been established for the 2006 PFS upgrade. A consultant initially hired to work on the upgrade, as well as various internal staff, used the login ID to implement the upgrade. The login ID was never deactivated even after the upgrade was complete. Audit notified the PFS system administrator that it should be deactivated, and the login ID has since been locked from the system.

Basic IT security controls specify that user IDs should be uniquely identified to specific users and their access rights to systems and data should be in line with defined and documented business needs. PFS allows login IDs to be blocked from the system without eliminating the login ID entirely. There may be times, such as during an upgrade, when a group login may be appropriate. Currently, a group login is used for accessing reports which is an example of an appropriate use of a group login. While it may be unlikely that a user login ID and password would be misappropriated for the purposes of fraud, the potential risk of a significant fraud is costly enough to warrant every precaution.

c. *A group login ID was used to allow an IS Developer rights in excess of his own login ID access rights.*

As stated above, one of the temporary user logins was created with high level access for use by a consultant and IS staff during the last upgrade. This login ID was never frozen from the system, even after the upgrade had been completed. An activity log showed that the user name was still in use, and Audit found that a developer in IS was using the login ID to conduct certain tasks that required greater rights than those provided through the developer's personal user ID. Audit was unable to determine who had given the IS developer the password in order to use the login ID.

The IS developer may have legitimate reasons to require more access rights than are currently provided (he does work on PFS on a regular basis). However, in the interest of access security controls, sharing of user names and passwords should be strictly forbidden. Furthermore, documentation identifying who provided the login ID to the IS developer as well as the authorized duration of access should have been maintained.

PFS Administrators have, at times, performed certain functional duties that violate segregation of duties standards and present a significant control risk.

PFS Administrators provide security administration as well as operational support for the PFS. In their role as operational support they at times perform certain functional duties. Audit found that PFS Administrators were editing vendor information for the HRA and Risk departments. Also, one of the PFS Administrators has been responsible for entering bank information for ACH payments during the pilot phase of the ACH implementation. PFS Administrators no longer have duties in Risk or HRA payments.

The PFS Administrators have super user access, including the ability to process payments. The ability to both change vendor information and process a payment is a fundamental segregation of duties deficiency. However, any functional responsibilities for the PFS Administrators present a serious control weakness. The Administrators have super user access which allows them to access and change data on practically any menu or panel. While the Administrators require high level access to be able to trouble shoot system problems, they should not take on functional responsibilities that do not fit with the authorized duties relevant to their position. Such functional duties bypass the traditional internal controls built into the system and position responsibilities as defined.

According to Control Objective PO4.11 in COBIT 4.1, personnel should only be performing authorized duties relevant to their respective jobs and positions. There should be a division of roles and responsibilities that reduces the possibility for a single individual to compromise a critical process. As a good business practice security administration should be separate from operational support.

If segregation of duties is not possible due to resource restrictions, then audit or exception reports and review processes should be set up to allow management to independently review system administrator actions; procedures should be implemented to ensure that such reviews occur.

The PFS System Developers have excessive user rights in the PFS production environment.

The bulk of the PFS System Developer's work is in the test and development environments and not in the production environment. The System Developer reported to Audit that he has higher level access rights than necessary for his duties. The Developers should need display level access in the production environment for the majority of their roles.

Currently the PFS System Developers have almost all the same high level access rights in the PFS production environment as PFS Administrators. These rights allow the potential for errors or fraud by the PFS System Developer, and put the Council at risk of efficiency and monetary loss. In order to limit the risk the Developer's access should be limited to display only in the production environment.

There isn't any comprehensive documentation of the assignment or termination of user access rights and roles.

All new users with access to production are set up by the PFS administrators. The types of rights required by the user are determined by the PFS administrator and the employee's manager. Discussions of user rights are generally done over email. Audit has not been presented with any of the user setup documentation, and the PFS administrator has indicated that sometimes it is hard to recall what a user login was created for. The PFS administrator does not keep consistent records of the users. There are close to 300 PFS users and it is not possible to control user access without an improved tracking system.

According to the Deputy CFO, the PFS administrators are expected to periodically review users and their associated rights with the appropriate managers. This review process is a key detective control in user access security. Currently the PFS administrators ask the employee managers if anything should be changed in terms of user rights. However, the managers are not provided with a list of which users they are being asked about nor are they provided with what the user's associated systems rights are. Audit found seven instances where user rights were associated with terminated employees. Five of the seven employees had been terminated for more than one year.

When job changes occur, especially job terminations, expedient actions must be taken to remove access rights so that risks are minimized. At the same time you may want to maintain a record of the access the user had. The PFS allows for users to be deactivated without eliminating the user from the system. By deactivating the user and not eliminating them from the system, you maintain the ability to see certain security data, such as user rights associated with the login ID.

According to Control Objective DS5.4 in COBIT 4.1, the system administrator should establish user management procedures that address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges. These procedures should include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be defined for all types of users. The system administrator should perform regular management review of all accounts and related privileges.

Password controls are in place.

Audit found that there were adequate password controls in place for PFS.

Password controls are turned on and configured for the following:

1. Password expiration.
2. Minimum password length.
3. Required special characters.

If a user forgets their password they are required to enter there user ID and then prompted with a question that they must answer correctly. Upon answering the question correctly they receive an email with a temporary password. When they log in to the system they are then prompted to create a new password.

Audit trails are not being utilized.

Discussions with the database administrator, the PFS administrators and the IS developers found that there are few, if any, audit trails that are activated and monitored within PFS.

An audit trail is a chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes. Audit trails, when turned on and monitored, are an important tool in managing the PFS. There are many audit trails that can be turned on. It is important to review what audit trails are needed and to activate only those which will be used and monitored.

The database administrator stated that he was learning about the security of the system and was not very familiar with the audit trails. The system administrators stated that they do monitor information on new vendors and vendor address changes. The IS developer had set up an audit trail on vendor address changes and new vendors but the system administrators said that it wasn't the one they use. Audit was unable to find a trail of the history of rights assigned to users. In general, there was a lack of information available concerning audit trails.

A lack of monitoring of changes made to the PFS increases the risk of financial and/or data loss. If auditing is not set or if the audit logs are not reviewed, unauthorized modifications to data and tables may not be identified and rectified on a timely basis. Consequently, data integrity and management reporting may be adversely affected. Once auditing is enabled, appropriate security should be enabled to prevent unauthorized alterations of the audit logs.

There is a lack of query security.

There are currently more than 2,100 public queries available to be used in the PFS. Public queries are those available to be used by any user with access to the Query Reporting Tool. In addition to the public queries there are also private queries that can only be used by the user who created the query. Although queries cannot modify data, inadequate security over queries has the potential to negatively impact system performance.

According to ISACA best practices, queries should be created on the development client and fully tested prior to implementation in the production environment. Users should have access only to run, not develop, queries on the production system. The PFS allows for predefintion of user query requirements which would allow for restricting users from creating queries on the production system.

The PFS administrators have stated that users are expected to create new queries in the test data base. However, there are no written procedures directing users to test the queries on the test data base. Inexperienced users may create and run poorly designed queries which could affect system performance. Currently processes are in place to shut down queries that may be impacting system performance.

Audit found other organizations that predefine commonly used queries along with providing instructions as to their usage. Definition and instructions in the use of common queries could help users more effectively utilize the query function by eliminating the need to search the 2,100 public queries for a query that will meet their needs.

Comparison of Support Staff

Audit requested information on IS support for financial and human resource systems from counties, large cities and school districts in the metropolitan area. Responses were received from five counties, three cities and three school districts. The information provided indicated that the Council's current level of system support is comparable to other local governmental units.

Data Flow

The PFS interfaces with the following Council information systems:

- PeopleSoft Human Resource Information System
- SPL(Synergen)- Environmental Service System
- TxBase- Metro Transit System
- Stars- Risk Management System
- Industrial Waste- Environmental Service System
- Capital Improvements- Environmental Services
- Disadvanged Business Enterprise- Office of Diversity
- HRA- Community Development

PFS is the Council's official financial system. Currently data flows between PFS and each of the eight systems. Two of the systems are financial systems. SPL(Synergen) is the Enterprise Asset & Work Management system used to integrate the needs of Maintenance, Inventory Management, Purchasing and Finance as well as timekeeping throughout Environmental Services. TxBase is the Maintenance and Materials Management system used to integrate the needs of Maintenance, Inventory Management, Purchasing and Finance at Metro Transit. SPL and TxBase are the original point of data entry for Environmental Services and Metro Transit respectively. A large part of IS time is spent on transferring data from SPL and TxBase into the PFS. This requires modifications to the formatting of the data prior to it flowing into the PFS. There is the potential that the data format for the two systems will not match which could impact financial reporting and decision making.

System Recoverability

Discussions with database administrators and PFS support staff indicate that basic processes are in place to ensure that the PFS is recoverable in the case of a disaster. It was reported to Audit that the PFS database is backed up everyday and stored on tape. In the case that the PFS fails, IS has several scripts for restoration scenarios. According to the DBAs, the scripts were tested once. IS support staff report that the system failed a few years ago and they were able to bring it back with relative ease. Each time an upgrade or patch is done to the system there is a restoration process that takes place. Also, discussions with IS support staff reveal that there have not been any data loss problems as a result of unexpected shutdowns of the system.

CONCLUSIONS

System Support and Functionality

Audit found that the majority of PFS users are satisfied with its functionality. Slightly more than half of the users who responded to the survey have had some training on PFS. Based on the responses to the survey there is a need for additional training, particularly in the area of Reporting Tools.

The majority of PFS users who receive help from the PFS support staff are satisfied with the help they receive. However, users located at Metro Transit generally seek help from inside their department. Based on interviews with Metro Transit users there is a value to having the PFS support staff available on site at Metro Transit.

System Controls

While there were good password access controls in place there were a number of system control weakness that were found. The weaknesses included the following:

1. There were limited but significant control weaknesses in the security of group login IDs.
2. PFS administrators have certain functional responsibilities that violate segregation of duty standards and present a significant control risk.
3. PFS System Developers have excessive user rights in the production environment.
4. There isn't any comprehensive documentation of the assignment of user access rights and roles.
5. Audit trails are not being utilized.
6. There is a lack of query security.

Support Staffing Levels

The number of support staff assigned the PFS and the HRIS system is comparable to other metropolitan area governmental units.

RECOMMENDATIONS

Program Evaluation and Audit recommendations are categorized according to the level of risk they pose for the Council. The categories are:

- **Essential –** Steps must be taken to avoid the emergence of critical risks to the Council or to add great value to the Council and its programs. Essential recommendations are tracked through the Audit Database and status is reported twice annually to the Council's Audit Committee.
- **Significant –** Adds value to programs or initiatives of the Council, but is not necessary to avoid major control risks or other critical risk exposures. Significant recommendations are also tracked with status reports to the Council's Audit Committee.
- **Considerations –** Recommendation would be beneficial, but may be subject to being set aside in favor of higher priority activities for the Council, or may require collaboration with another program area or division. Considerations are not tracked or reported. Their implementation is solely at the hands of management.

1. PFS administrators must develop a system to maintain documentation of all PFS users as to the purpose of their access and assigned rights as well as ensure that access is terminated when the user no longer requires access. This system should align with COBIT 4.1, Control Objectives DS5.3 andDS5.4. (Essential)

According to Control Objective DS5.3 in COBIT 4.1, all users should be uniquely identifiable, and their access rights to systems and data should be in line with defined and documented business needs; job requirements should be attached to user identities.

Control Objective DS5.4 in COBIT 4.1, states that the system administrator should establish user management procedures that address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges. These procedures should include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be defined for all types of users. The system administrator should perform regular management review of all accounts and related privileges.

Management Response: Existing procedures for granting system access will be augmented to include annual verification of access rights by supervisors. Users who have not accessed the system have had their access rights terminated. Most users had inquiry only access rights given to them at implementation. Availability of standard reports on the Council's Intranet has eliminated the need for inquiry access for many users.

Users currently have a unique user id and are assigned access rights in security profiles established for the functions they need to perform. A log will be maintained to track future new users and changes to user profiles. The log will contain fields for user name, user id, security profile, supervisor, and date requested.

Staff Responsible: Mary Bogie *Estimated Complete: May 2009*

2. Finance must address the significant control weaknesses caused by the deficiency in segregation of duties for PFS Administrators. (Essential)

The PFS administrators have super user access to the system, and at the same time they have performed certain functional duties that could compromise the Council's systems of internal control over disbursement of funds. According to Control Objective PO4.11 in COBIT 4.1, personnel should only be performing authorized duties relevant to their respective jobs and positions. There should be a division of roles and responsibilities that reduces the possibility for a single individual to compromise a critical process.

If segregation of duties is not possible due to resource restrictions, audit trail or exception reports should be set up to allow management to independently review system administrator actions.

Management Response: Financial system support staff do not routinely perform operating functions. Responsibilities for vendor access during the pilot phase of implementing electronic payments to vendors were assigned in order to control the environment under which the project rolled out. Responsibilities have since been re-assigned to other staff.

Because financial system support staff require "super user" access rights to the system, additional audit trails (queries of system transaction and table updates) will be run and reviewed monthly for appropriateness.

Staff Responsible: Mary Bogie *Estimated Complete: May 2009*

3. Management should address PFS IS developers access rights in the production environment. (Significant)

The PFS IS developers have been granted high level rights in the production environment. They should have the high level rights in the development and test environments only. In the production environment they require a read only access. If additional rights are required in the production environment they should be granted for the time period that they are needed only. If the rights are required in order to back up the PFS administrators, the number of IS people with rights should be reviewed.

Management Response: Access rights of IS development staff have been limited to inquiry only for the production environment.

Staff Responsible: Larry Howieson   Estimated Complete: May 2009

4. Appropriate audit trails should be activated and used to improve monitoring of system transactions. (Significant)

Audit found one high level generic user ID that was being used by an IS Developer. Neither the PFS administrators, nor the database administrator were able to determine who had given user ID and password to the IS developer. Audit also found that there wasn't historical user data available for user IDs assigned to employees who were recently terminated from the Council and the PFS. The database administrator said that he was learning about PFS system security and was not aware of what audit trails were activated.

Both the PFS system and database administrators have the ability to grant security access to the system. There should be an audit trail in place identifying who they are giving rights to. Reports should be produced and monitored to ensure that the assignment of the rights is in line with Council business purposes.

Audit trails if they are in place are only of use if the information produced from the audit trails is reviewed by appropriate people. Audit trail reports could be used to monitor transactions by users who may violate segregation of duty standards, among other key control issues.

Management Response: Staff will review audit trail reports available in the system to determine benefit and implement where appropriate.

Staff Responsible: Mary Bogie, Larry Howieson   Estimated Complete: June 2009

5. PFS security administrators should consider using automated security diagnostic tools for application security assurance and data integrity assurance. (Consideration)

System security can take a significant amount time. With the number of other system support responsibilities assigned to the PFS administrators, key security exposures can occur. Automated security diagnostic tools are needed to:

- Provide a historic view, e.g., identifying when security parameters were changed
- Unravel complex security profiles
- Provide dynamic documentation of user access
- Promote independence (i.e., permissions are developed independently to access the required data)

- Be noninvasive (i.e., there is minimal disruption to the operation of the production system, usually through extracting and downloading the required information offline for subsequent evaluation)

Third party tools are also available that can provide real-time preventive controls so that as access is granted to new or existing users, automated checks against their segregation of duty tables are executed, which may prevent inappropriate access from being granted. These tools can:

- Identify potential control issues
- Route the details to the appropriate individuals
- Capture corrective action plans
- Monitor progress over time in addressing the issue.

These types of tools help support and enable compliance.

Management Response: Staff will consider this option. The cost of automated diagnostic tools may be excessive given the size/scope of the Council's application.

Responsible: Mary Bogie, Larry Howieson *Estimated Complete: Dec 2009*

6. Management should assign PFS security duties to an individual who is not charged with functional support. (Significant)

As a good business practice the PFS security administration should be restricted to security administration of the system and maintaining user access as requested by data owners. The security administration should be separate from functional system support in order to maintain segregation of duties controls. Currently most Council system security administration is handled in the IS department.

Management Response: Financial system support staff are not normally tasked with performing operating functions and thus are appropriately assigned security functions. As discussed in management's response to recommendation #2, audit trails will be run and reviewed monthly as compensating controls to address the audit concern for segregation of duties.

Responsible: Mary Bogie *Estimated Complete: May 2009*

7. Management should consider implementing systems to make the use of PFS queries more efficient for system users and overall system performance. (Consideration)

According to IS best practices, system users should be restricted from creating queries in the production environment as badly designed queries can negatively impact system performance. In the past, Council management has made the decision to allow PFS users to create and run public queries as needed in the production environment. Currently, the PFS has over 2,100 public queries available for use.

Audit recommends that management should consider restricting access to create queries in the production environment in order to better align with industry best practices. Additionally, Audit recommends that management consider improving the organization or systems for accessing public queries so that users can more easily identify common queries for use.

Management Response: Query access is intended to meet the ad hoc reporting needs of users. Queries that are impacting performance are terminated by support staff. Management will consider additional avenues (see management response for recommendation #8) for training related to creating and organizing queries to address the audit concern.

Staff Responsible: Mary Bogie Estimated Complete: Dec 2009

8. Training plans should be developed on an annual basis to ensure that user training needs are addressed. (Significant)

It is a prudent business practice to ensure that users of an enterprise system such as PFS should be properly trained on its function. Proper training on the capabilities of the PFS will result in better utilization of the system and in turn increased productivity. Many of the survey respondents receive assistance with PFS from coworkers within their own departments who may not fully understand the PFS. This creates the potential for the use of incorrect or inefficient procedures to become the standard process. If the PFS administrators seek input from the various users they can then offer training in those areas that the users have specified the desire for training in.

Management Response: Transactional users of the financial system are centralized in the accounting areas of Regional Administration and Metro Transit. Users receive one-on-one training from financial system support staff or staff in their areas with knowledge of transaction entry. Financial support staff are also available to other users to support query and reporting functions on a one-on-one basis.

Staff will develop a communication plan to address availability of training and increase content available on the Council's intranet to address functionality, best practices, and frequently asked questions.

Staff Responsible: Mary Bogie Estimated Completion: Dec 2009

9. On a periodic or as needed basis, the PFS administrators should meet with users with common roles on the PFS to discuss PFS issues. (Consideration)

Within the PFS users are assigned various roles. In many instances these roles will cross over between the various divisions within the Council (i.e., accounts receivable RA, accounts receivable Metro Transit). Communications between the various divisions is often infrequent or at levels higher than the average user. By meeting together and bringing issues or problems that they are encountering with the PFS the users may learn better ways of addressing the issues or find that solutions already exist. This will result in a more efficient use of Council resources.

Management Response: Staff at appropriate levels already meets on a periodic basis. Meetings are currently held to discuss new functions/processes expected in software upgrades, operating procedures, and issue resolution. Staff levels range from data entry to manager where appropriate.

APPENDIX A

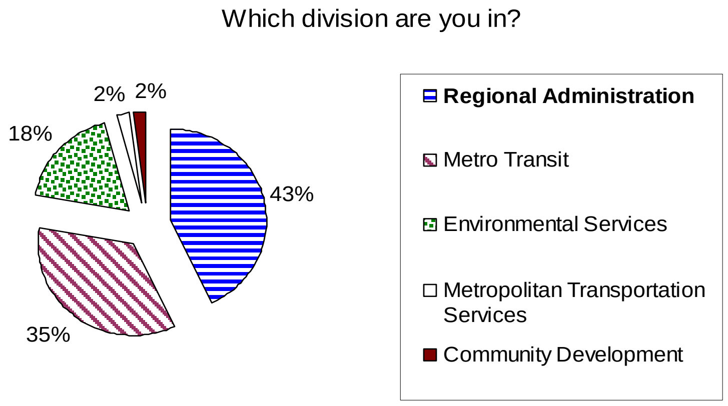
PeopleSoft Financial System (PFS) User Survey

Audit conducted a survey of 248 Council employees who have access to PFS. PFS users were surveyed on their use of the system, training opportunities and help with system questions, and user satisfaction with the PFS overall.

A total of 99 employees participated in the survey representing a 40% response rate. Four of the surveys were deemed “incomplete” because they lacked sufficient responses bringing the final response rate to 38%. An additional seven employees responded by email that they never use the system.

The survey participants were asked to identify the area of the Council in which they worked. Graph 1 shows the breakdown of responses. The largest percent of respondents, 43%, were from Regional Administration while Metro Transit represented 35% of the respondents. Audit received very few responses from Metropolitan Transportation Services and Community Development.

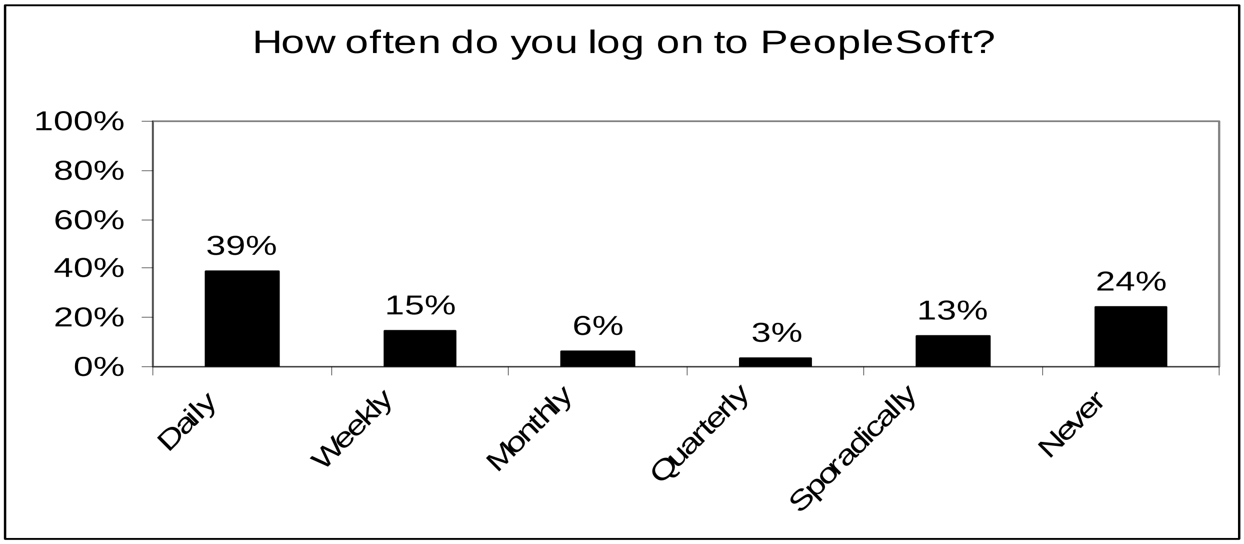
Graph 1:



Frequency of PFS Use

As Graph 2 shows, the largest percentage of respondents, 39%, reported using the PFS daily. However, 24% reported *never* using the PFS and this was the second most common answer on frequency of use.

Graph 2:



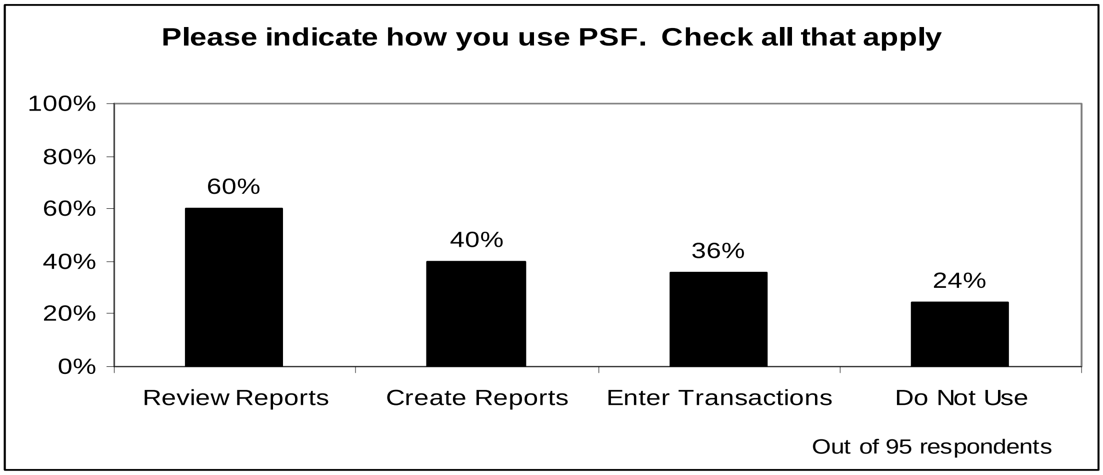
Out of 95 respondents

Audit also asked users about accessing the PFS from locations other than their normal work station. For example, some PFS users can access the system from their home computer via the Citrix system. Only 6% of respondents reported accessing the system from a remote location.

Commonly Used PFS Modules and Functions

In general, most respondents reported using the PFS to review reports (see Graph 3). PFS users were also asked to indicate the specific modules and functions they use in the PFS. Modules include general ledger, accounts payable, accounts receivable, asset management, vendors, billing, and reporting tools. Reporting tools was the most commonly used module with 50% of respondents indicating that they use reporting tools. The reporting tools function includes multiple capabilities, but most respondents reported using reporting tools to access an existing query.

Graph 3.



Accounts payable and general ledger modules were also reported as commonly used; 46% and 43% of respondents indicated using accounts payable and general ledger modules, respectively. Table 1 includes the reported use for all modules.

Table 1. Which PFS modules and features do you use?

	#	%
General Ledger	40	42.6%
Accounts Payable	43	45.7%
Accounts Receivable	19	20.2%
Asset Management	11	11.7%
Vendors	24	25.5%
Billing	15	16%
Reporting Tools	**47**	**50%**
Unknown	2	2.1%
None	22	23.4%

PFS and Other Applications

As stated in the audit report, the PFS interfaces with a number of Council systems. Survey respondents were asked to indicate other systems they use to supplement the PFS. Along with other systems that interface with the PFS, users were asked about Microsoft Office programs that they use to supplement the PFS. The most common systems that users access to supplement the PFS include Microsoft Excel and Word, PeopleSoft HRIS, Synergen and Txbase.

Table 2. What other applications do you use to supplement the PFS?

	#	*%*
PeopleSoft HRIS	25	27.5%
Excel	**57**	**62.6%**
MS Word	27	29.7%
MS Access	7	7.7%
Synergen	24	26.4%
Txbase	23	25.3%
Capital Improvements	5	5.5%
DBE	4	4.4%
HRA	5	5.5%
Risk	10	11%
Industrial Waste	5	5.5%
None	20	22%

PFS Training

The PFS User Survey asked respondents to indicate any past training, satisfaction with past training, and any future training needs. A little over half, 53%, of respondents indicated that they have received some training; 47% of respondents indicated that they have received no training.

Audit asked PFS users to indicate from whom they received training. Respondents were given the training options of internal PFS support, external classes, co-worker, and other. Internal PFS support is made up of two Business System Analysts who are also the administrators for the PFS. Respondents indicated receiving most training from internal PFS support. Forty-one percent of respondent training came from internal PFS support; respondents also indicated receiving 35% of training from co-workers.

Respondents were asked to indicate the PFS modules for which they received training. Most respondents indicated receiving training on reporting tools, accounts payable and general ledger modules.

Table 3. Training Types and Sources

Training Type/Module	Internal PFS Support	External Classes	Coworker	Other	Total	%
fit gap	9	1	0	0	10	5.7%
general ledger	9	6	11	1	27	15.4%
accounts payable	15	4	12	2	33	18.9%
accounts receivable	3	3	7	0	13	7.4%
asset management	3	6	1	0	10	5.7%
vendors	6	2	7	1	16	9.1%
billing	5	1	5	0	11	6.3%
reporting tools	14	9	13	1	37	21.1%
query builder	8	3	5	2	18	10.3%
total	72	35	61	7	175	
%	41.1%	20.0%	34.9%	4.0%		

The vast majority of respondents, 60%, report being satisfied or very satisfied with the training they have received. Only 18% of respondents reported being dissatisfied with training. The survey asked dissatisfied respondents to elaborate on their response. Comments included:

- "I would like an opportunity to get basic functional training so I know why I'm putting entries into fields instead of "click" here & there."
- "This is my biggest frustration. We have spent a lot of money on PeopleSoft and yet there is NO manual and NO training. I can virtually not use the system for my needs because what little training I have received has only given me limited capabilities. If the Council wants to get the most out of the money it has spent on what looks to be a pretty good system, we should get some training and some manuals for reference on things we do infrequently."

PFS users were asked to indicate any areas in which they would like additional or refresher training. While the largest percentage of respondents (42%) indicated that they do not want any further training, a significant number of respondents indicated that they would like additional training in reporting tools (33%) and query builder (35%). Some users also indicated that they would like further training in general ledger and accounts payable functions.

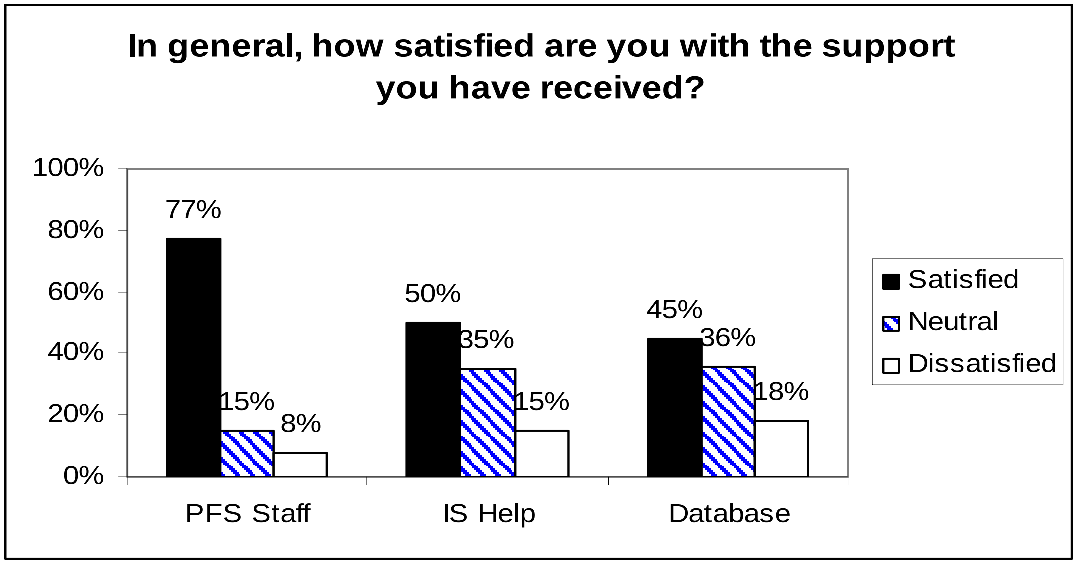
PFS Help

Audit asked PFS users to indicate from whom they received assistance when they have questions on the PFS. The survey asked respondents about a range of possible support options including internal PFS support, the IS help desk, co-workers in the users' department or other departments, and database administrators. Respondents also had the option of reporting that they do not access any of the listed sources of help.

Most respondents reported receiving assistance from internal PFS support and from co-workers in their department most often. Thirty-five percent reported receiving help from co-workers in their department most often, while 38% reported receiving help from internal PFS support most often. In general, PFS users do not use the IS help desk for assistance with the system.

The survey asked respondents to rate how satisfied they are with the assistance that they have received. While respondents could rate assistance received from the IS help desk and DBA's, internal PFS support is supposed to be the main source of system assistance. Respondents reported being very happy overall with the assistance they have received from internal PFS support; 77% of respondents reported being satisfied or very satisfied with internal PFS support and only 8% reported being dissatisfied with past assistance. Graph 4 illustrates respondent satisfaction regarding PFS assistance.

Graph 4:



User Satisfaction with PFS Performance

PFS users were asked to rate their overall experience with the system in the following categories: ease of use, online help, processing speed, convenience, availability, reports, and overall. Most users reported being satisfied or very satisfied in almost all of the categories. Online help was the only item that did not receive a satisfied rating from most respondents; 65% of PFS users reported neutral feelings toward online help. Respondents reported being most satisfied with system availability and PFS reports. Almost 50% of respondents reported being satisfied or very satisfied with overall system performance.

Respondents who indicated dissatisfaction with any aspect of PFS performance were asked to provide any comments that could elaborate on their dissatisfaction. Comments included:

- “Can be very slow at times. Not all the time, but is very frustrating when trying to beat a time-line before matching jobs etc.”
- “The online help seems very complex and therefore it isn’t user friendly. It appears to be best suited to the support staff rather than the average user.”
- “I find PeopleSoft to be cumbersome to use which may just be my lack of understanding on how the system works. There have been several changes made to the system and I was out of work for over a year, so I am totally confused at this point.”

Lastly, respondents were asked to provide any additional comments on the PFS. Most of these comments expressed a desire for training and other opportunities to gain further understanding of the PFS and its capabilities. For example, respondents wrote:

- “It would be useful to have a summary of what PeopleSoft does and what information is available.”
- “Offer training on a regular basis would be nice. The last one that I signed up for, I couldn’t attend due to medical reasons.”

Of the ten additional comments provided by respondents, six indicated a desire for further explanation and training on system capabilities.