

OFFICE OF AUDITOR GENERAL



PeopleSoft Financial System Controls
Audit Report

May 28, 2009



PS Financial System Controls Index

<u>Report Section</u>	<u>Pages</u>
Executive Summary	1
Summary of Recommendations	3
Observations, Recommendations and Action Plans	
Monitoring Essential Processes	4
PeopleSoft Updates	5
Operating Procedures	6
Query Table Access	8
Passwords	9



PS Financial System Controls Executive Summary

OBJECTIVE

To evaluate the Financial System Controls in PeopleSoft 8.9 for propriety and sufficiency to generate accurate financial reporting and enable fiscal accountability.

BACKGROUND

The PeopleSoft system is an enterprise-wide system that was implemented to automate and streamline operations. The District implementation date for the upgrade from PeopleSoft 8.4 to 8.9 was July 18, 2007. The conversion included Accounts Payable, General Ledger, Budgets, Purchasing, Projects, Asset Management, Grants and Contracts. An additional module, eProcurement, and the functionality of Workflow were added to the implementation. Increased functionality of the new environment was provided to improve system use District-wide, the internal control environment and return on investment.

Financial transactions of the District are gathered by departments via spreadsheets and PeopleSoft modules. This data is then summarized in the PeopleSoft General Ledger for financial reports to management and other interested parties.

SCOPE

Our audit will evaluate the effectiveness of internal controls, records management, and procedures over Financial Reporting in PeopleSoft.

We will:

- 1) Assess existing PeopleSoft application controls and design for effectiveness and efficiency.
- 2) Review User roles, permissions, profiles workflow and manual authorization controls for reasonableness.
- 3) Assess reliability of reports and queries used to compile and communicate financial results to internal and external parties.
- 4) Evaluate procedures to monitor application changes for sufficiency and ensure system integrity.

We rely upon key personnel and their designees to develop our understanding of the current control environment. We will then test the identified controls and assess their effectiveness. Results of our audit procedures will be summarized to determine internal control concerns and provide recommendations to improve the control environment. Management will be requested to respond to our recommendations, in writing, for inclusion in our final report to management and the Board of Education.



PS Financial System Controls Executive Summary

CONCLUSION

IM&T operating practices regarding the sharing of information and decisions with business owners could be enhanced. Opportunities exist regarding notification of key automated process failures and communication of potential problems and fixes from PeopleSoft. While some PeopleSoft processes are complex and IM&T has some documentation, the operating procedures and design documentation are not adequate to ensure IM&T operational continuity in the event of staff turnover. This level of documentation also restricts other District departments in their understanding of key automated processes. Additionally, the password controls are weak and District guidelines have not been formalized to direct a desired level of control. Weak password controls could allow improper access to sensitive data (personal or otherwise) housed in PeopleSoft but accessible through public queries.



PS Financial System Controls Summary of Recommendations

Rec#	Recommendations
1	<i>Review, document, and monitor automated processes with business owners to determine essential business functions that should be monitored if process failures exist. Communicate essential process failures when they occur.</i>
2	<i>Review current patch component fixes with functional managers during existing monthly meetings.</i>
3	<i>Document IT operating procedures. Document PS application technical design configurations and purposes for options currently being utilized. Develop and implement a change control operating procedure to ensure changes are accepted in writing and achieve the desired business objective.</i>
4	<i>Work with process owners to identify data tables with sensitive data and determine appropriate user access. Use PeopleSoft query security controls to align RCSD PeopleSoft users to have access to information necessary for their job performance.</i>
5	<i>Implement and communicate stronger password controls. Require the policy to be reviewed periodically for appropriateness.</i>



PS Financial System Controls Observations, Recommendations and Action Plans

OBSERVATION #1

Monitoring Essential Processes

Formalized monitoring procedures for essential processes have not been established with process owners. IM&T developers receive automated e-mails when processes fail. Currently, developers determine when it is appropriate to communicate the failures to process owners. Operating management relies on consistent performance of automated activities to provide a first level of control in the financial systems. Operating management cannot rely on timely communication from IM&T if an understanding of essential processes and related monitoring has not been established and agreed upon. As a result, delays in corrective action can occur should an automated activity not complete properly.

RECOMMENDATIONS and MANAGEMENT RESPONSES

Review, document, and monitor automated processes with business owners to determine essential business functions that should be monitored if process failures exist. Communicate essential process failures when they occur.

Management Responses:

All currently monitored processes will be reviewed with Business Owners. If the Business Owners wish to be included on the Distribution Lists to receive an automated email if a process fails, they will be added to the Distribution. When reviewing these processes with the Business Owners, if there are any additional processes identified for which monitoring would also add value, monitoring will be established for these processes, as well.

Responsibility: Jerome Underwood, Technology Information Officer; Annmarie Lehner, Manager of Technology Services

Due Date: December 31, 2009



PS Financial System Controls Observations, Recommendations and Action Plans

OBSERVATION #2

PeopleSoft Updates

IM&T communicated that PeopleSoft patches are posted on Oracle's web site and those patches are available to all customers including RCSD users. Given that availability, IM&T states they do not proactively communicate reported issues, or known repairs to RCSD business owners because they do not have the resources to do so. The District practice is to hold all PeopleSoft notices for an annual, mass installation. This practice is utilized to better align with available resources. Repairs for improperly working functions that the user may not be aware of, or has not communicated to IM&T, can go uncorrected until year end. As a result, system or user operating inefficiencies can occur and end users miss the opportunity for consideration of earlier correction.

RECOMMENDATIONS and MANAGEMENT RESPONSES

Review current patch component fixes with functional managers during existing monthly meetings to improve awareness and resolution to repairs.

Management Responses:

The maintenance of the PS Financials application is performed annually January thru April to coincide with the schedule of our Business Owners who must test the system. As there were 1,011 patches created in the maintenance applied last year alone (a 10-month period of time), it is not feasible to review all patches with our Business owners – even on a monthly basis. Business owners do test all Production processes and reports after any and all maintenance is applied to make sure there are no negative impacts resulting from all changes made, even though not patch specific. A comprehensive test plan has been created for this purpose and this is updated annually with input from the Business Owners. They are required to sign-off on testing performed which is retained for review. IM&T management has accepted this process as adequate and the Business Owners have also accepted this standard of applying maintenance on an annual basis. We will formalize this maintenance agreement by defining and documenting our process, its user approval, and clarify business owner responsibilities, including awareness and acceptance for all software changes as noted on the web site and associated testing risks when installed.

Responsibility: Jerome Underwood, Technology Information Officer; Annmarie Lehner, Manager of Technology Services

Due Date: December 31, 2009



PS Financial System Controls Observations, Recommendations and Action Plans

OBSERVATION #3

Operating Procedures

PeopleSoft applications are highly complex and configured to accommodate specialized needs of the District. Procedures and functionality, as designed, should be documented to ensure operational continuity independent of IT personnel. Examples OAG believes should be included are:

- Specific application functions that are enabled and associated customizations including, but not limited to, combination edits, workflow, security, matching, external and internal interfaces.
- Technical monitoring processes and tools used to ensure system integrity.
- Change Control procedures and proof of user acceptance.
- User access and security procedures to maintain the system.

IM&T was unable to provide documented PeopleSoft application configurations and operating procedures. They also do not have complete or formally documented design configurations or IM&T operating procedures for PeopleSoft financial applications used by the District. Discussions with IT staff indicated that IT operating practices do exist. Some IM&T staff members provided developer notes for OAG to derive an understanding of documented PeopleSoft processes and controls; however these documents were not comprehensive.

IM&T's ability to maintain PeopleSoft applications may be hindered through staff transition. In addition, cross training should occur to ensure RCSD's operating processes are not hindered during transitions. Improper or unauthorized changes could be made to PeopleSoft applications due to lack of documented configurations, policies and procedures.



**PS Financial System Controls
Observations, Recommendations and Action Plans**

RECOMMENDATIONS and MANAGEMENT RESPONSES

Document IT operating procedures. Document PS application technical design configurations and purposes for options currently being utilized. Develop and implement a change control operating procedure to ensure changes are accepted in writing and achieve the desired business objective.

Management Responses:

IM&T will review internal functions to assess where there may be inadequate documentation and based on criticality of need, IM&T will document any areas identified. We agree that change control procedures and some security operating procedures qualify. IM&T will review and revitalize the previously-utilized change control procedures and will communicate this process to Business Owners.

Responsibility: Jerome Underwood, Technology Information Officer; Annmarie Lehner, Manager of Technology Services

Due Date: March 31, 2010



PS Financial System Controls Observations, Recommendations and Action Plans

OBSERVATION #4

Query Table Access

All District data in PeopleSoft are housed in data tables viewable by all PeopleSoft users via Query Report Writer. IM&T does not utilize PeopleSoft delivered security controls to restrict user access to query tables containing sensitive data. Some examples of tables containing sensitive data that have unrestricted access and are visible to users are the "1099 Vendor Table" in PeopleSoft Financials that contains visible vendor tax ID numbers and social security numbers. There are 24 public queries providing this information and over 200 employees with access to it. Additionally, in the PeopleSoft Human Resource system, the "DEPT_SALARIES_NVISION", the Department Salaries table, contains visible employee salaries.

Access to sensitive data housed in PeopleSoft should be restricted to users based upon their job functions. Information protected under regulatory privacy laws should be maintained in compliance with those standards. Sensitive information such as tax payer ID's and social security numbers can be accessed and used for unauthorized purposes.

RECOMMENDATIONS and MANAGEMENT RESPONSES

Work with process owners to identify data tables with sensitive data and determine appropriate user access. Use PeopleSoft query security controls to align RCSD PeopleSoft users to have access to information necessary for their job performance.

Management Responses:

Only Business Owners "super users" have access to Query Manager – allowing them to create queries of their own. This access level has been approved by their managers and this access is reviewed with management on an annual basis.

Other users of the Financial System have access to Query Viewer, which allows them to run Public Queries only. IM&T will review, with the Business Owners, the public queries that are available and will restrict those queries that contain sensitive information. Since we currently have 2,362 public queries, this process will take a significant amount of time to complete.

Responsibility: Jerome Underwood, Technology Information Officer; Annmarie Lehner, Manager of Technology Services

Due Date: June 30, 2010



PS Financial System Controls Observations, Recommendations and Action Plans

OBSERVATION #5

Passwords

[REDACTED] A password control policy has been drafted and IT is in the process obtaining approval from various process owners. There is no expected date for its completion; however a draft has existed for several years.

Password controls should be designed with enough complexity to serve as a reasonable deterrent for unauthorized users seeking to gain access to PeopleSoft. Password controls are the key to a person's identity on the system and should be reasonably designed to protect that identity.

RECOMMENDATIONS and MANAGEMENT RESPONSES

Implement and communicate stronger password controls. Require the policy to be reviewed periodically for appropriateness.

Management Responses:

Once the District's overall Password Control Policy has been approved by management, the new controls will be applied to the District's PeopleSoft applications. Password Policy requirements have been discussed with the Deputy Superintendent of Administration. This level of management is required to roll out a new password policy throughout the District. Follow-up on this subject is on-going.

Responsibility: Jerome Underwood, Technology Information Officer; Annmarie Lehner, Manager of Technology Services

Due Date: January 31, 2010