PEOPLESOFT HUMAN RESOURCES AND PEOPLESOFT FINANCIALS SYSTEM CONTROLS REVIEW

PROGRAM EVALUATION AND AUDIT

METROPOLITAN COUNCIL

November 2017

INTRODUCTION

Background

At the Metropolitan Council (the Council), PeopleSoft Human Resources (PS HRMS) and PeopleSoft Financials (PSF) contain complex databases that hold financial and personnel information. These systems make it possible to work with data and route it to and from business operations around the Council. The two systems share information with each other and serve as an information exchange for a host of business systems that keep the Council running smoothly and efficiently.

Purpose

The purpose of this audit was to identify potential risks and weakness with in controls as well as identify solutions to mitigate risks and strengthen controls. This was considered through the Thrive MSP 2040 lens. In accordance with the Thrive MSP 2040 principle of accountability, "results matter, and for the Council, accountability includes a commitment to monitor and evaluate the effectiveness of our policies and practices."

Scope

The audit included a review of user roles and responsibilities and system access controls. The review was limited to the production environment for both systems. Additionally, Audit only reviewed users not locked from the system.

Methodology

Data Collection

Interviews were conducted with:

- Finance department staff.

The following information was reviewed:

- System access controls.

Evaluation

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

- Password requirements.
- Assignment of roles.
- User rights.

Assurances

This audit was conducted in accordance with the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing and the U. S. Government Accountability Office's Government Auditing Standards.

OBSERVATIONS

System Controls

Security administration functions control the access to the application and data stored within the PSF and PS HRMS systems and support the confidentiality and integrity of the data. Access to the applications is defined by the assignment of user IDs to various roles within the system. Within the roles a user has permission lists and menu items that are assigned to them with varying levels of access. Audit reviewed user IDs and the roles assigned to them for both systems for appropriateness and reasonableness for users in similar jobs.

Password controls are in place

Audit found there are adequate password controls in place for both systems. The password parameter settings follow the Council's password procedure.

Controls in place regarding use of group login IDs

Most PeopleSoft users are granted access to either system with an individual login ID. The access rights attached to that login ID should be appropriate to the individual's position as determined by their manager and the PeopleSoft administrator. Audit identified 18 login IDs in the PeopleSoft systems that were not for individual people but for other purposes. PeopleSoft administrators provided the purpose of the login and the users with knowledge of the password.

There is timely removal of user access

Audit found an auto generated report sent to the PeopleSoft administrators that indicates staff that have recently been terminated. The administrators are then able to use this information to lock users from either system should they have had access during their employment with the Council. Further, on a yearly basis, PeopleSoft administrators verify with managers, via email, that their direct reports' access to either PeopleSoft system is relevant to their job function.

Procedures in place for granting access

Audit found procedures exist on processing PeopleSoft security request forms including procedures on creating user profiles in PSHRMS and PSF and determining access required.

Documentation is not in place defining roles used in PeopleSoft HRMS

Documentation is not in place defining the roles, permission lists, menus and pages required for different job functions within the HR and Payroll departments and other departments that use PS HRMS. This documentation does exist for PSF, however, there is not a procedure for maintaining the documentation. According to Control Objective DS5.3 in COBIT 4.1[1], user access rights to systems and data should be in line with defined and documented business needs and in keeping with best practice, the roles used in PS HRMS should be documented. Without the detailed documentation of how roles were developed and implemented, it may be difficult to adequately monitor and system access rights. Additionally, without the documentation, it is difficult to determine whether security has been implemented to maintain segregation of duties. Per conversations with the Senior Manager of Administrative Systems Support, she simply had not had a chance to document the roles in PS HRMS.

Information services developers potentially have excessive user rights in the PeopleSoft HRMS environment

Certain information services (IS) developers have access rights which seem to be in excess of what is needed for their roles. Additionally, there is overlap in many of the roles assigned to IS with the roles assigned to the PeopleSoft administrators. According to Control Objective DS5.3 in Cobit 4.1[2], user access rights to systems and data should be in line with defined and documented business needs. Having production rights in excess of those needed by system developers increases the risk of errors or fraud.

[1] The IT Governance Institute (ITGITM) was established in 1998 to advance international thinking and standards in directing and controlling an enterprise's information technology. ITGI designed and created COBIT® 4.1 as an educational resource for chief information officers (CIOs), senior management, IT management and control professionals.
[2] Ibid.

CONCLUSIONS

Audit found there to be adequate controls with regards to password requirements, assignment of roles and user rights. There are opportunities for implementing additional controls including documenting the roles assigned to users in PeopleSoft HRMS. Additionally, the user rights of IS developers in PeopleSoft HRMS should be reviewed for relevancy.

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.
- **Verbal Recommendation –** An issue was found that bears mentioning, but is not sufficient to constitute a control risk or other repercussions to warrant inclusion in the written report. Verbal recommendations are documented in the file, but are not tracked or reported regularly.

1. **(Significant) As a best practice, and like the documentation for PeopleSoft Financials, administrative systems support should document the roles used in the PeopleSoft HRMS system.** Additionally, procedures should be documented on how to maintain the document including for PeopleSoft Financials.

   Management Response: *We concur with this best practice as it creates a more user-friendly understanding of the access rights assigned to individual users.*

   Staff Responsible: *Chi-yi Chou, Administrative Systems Support Manager*

   Timetable: *First Quarter, 2018*

   Thrive 2040 Principles: *Accountability.*

2. **(Significant) The access of IS Developers in the PeopleSoft systems should be reviewed for appropriateness.** Administrative systems support should continue to review access periodically and additionally review after system upgrades.

   Management Response: *We concur with this recommendation and have already reviewed and tightened current access rights for our IS Developers. We will also confirm necessary access rights that are granted during system upgrades are relinquished as appropriate upon project completion.*

   Staff Responsible: *Chi-yi Chou, Administrative Systems Support Manager*

   Timetable: *Complete*

   Thrive 2040 Principles: Accountability.

METROPOLITAN
COUNCIL

390 Robert Street North
Saint Paul, MN 55101-1805

651.602.1000
TTY 651.291.0904
public.info@metc.state.mn.us
metrocouncil.org