Minneapolis
City of Lakes

PeopleSoft Finance Access and Security Audit

City of Minneapolis – Internal Audit Department
September 20, 2016

Minneapolis
City of Lakes

Contents **Page**

Minneapolis
City of Lakes

Internal Audit Department
350 South 5th Street, Suite 302
Minneapolis, MN 55415-1316
(612) 673-2056

Date: September 20, 2016

To: Mayor Betsy Hodges, City Council Members, Chief Information Officer Otto Doll, Chief Financial Officer, Mark Ruff and City Coordinator Spencer Cronk

Re: PeopleSoft Financials Access Audit

Background

The City of Minneapolis (City) uses the PeopleSoft Enterprise Resource Package (ERP) software to support their Finance department operations. The Finance functions manage confidential and sensitive data such as social security numbers, tax identification numbers, personal wage garnishment, vendor and personal banking information to name a few. The City's Internal Audit department conducted a review of the PeopleSoft application in collaboration with PeopleSoft Support and the IT Department.

Objective, Scope and Approach

The PeopleSoft Finance application (COMET) was upgraded in 2015. Processes and role design post upgrade were reviewed as part of this audit. Internal Audit conducted interviews with the responsible and accountable people in order to gain an understanding of the role design, system work flows and access management procedures. System generated role and user profiles were obtained to analyze the data for segregation of duties conflicts. Payment vouchers were also analyzed to note compliance with the 3-way match processes and to identify any duplicate payments. Please refer to the Procure to Pay audit for further details and testing on the 3-way match and procurement procedures. Testing of user on-boarding and terminations for the COMET application were performed by the state auditors in 2016. Please refer to their testing for user access administration controls on on-boarding and terminating user access. Access to the PeopleSoft application is via the Web Portal, which was separately evaluated in 2016 as part of the Web Portal Audit; please refer to the Web Portal audit report for further testing details and results.

The objective for this audit is to review system access to note potential segregation of duties conflicts and privileged access management practices. The scope included:

- Functional end-user access for segregation of duties across treasury, purchasing, inventory, fixed assets and general ledger roles.
- Procedural and systematic enforcement of privileged access via both the front end through the application and the back end through direct database or operating system access.

Audit Results and Recommendations

Finding 1: Segregation of Duties

The American Institute of Certified Public Accountants (AICPA) recommends that activities relating to authorization, custody of the assets and recording transactions be segregated in order to prevent unauthorized or inappropriate access or loss of data and assets. We performed an analysis at the role and user levels to note if there are any potential segregation of duties conflicts and identified such a scenario in inventory management.

In Inventory Management the role M_UPDATE_STOCK_INVENTORY has the ability to add, modify and delete inventory records, reconcile the inventory records to physical counts and record adjustments to the inventory records in the General Ledger(GL). Having the ability to record inventory records and authorize the reconciliation of the inventory in the same role creates a potential risk for loss of assets without an audit trail. There are two users who had this role assigned within the COMET system.

Segregation of Duties – Recommendation

We recommend segregating the access to record inventory in the system from the ability to reconcile against physical counts and record adjustments in both inventory and General Ledger accounts. This will help lower the risk of loss of assets as the same individual who maintains inventory would not be responsible for counting and reconciling the inventory records.

Segregation of Duties – Information Technology Response

The inventory business function and transactions will be moving to the MAXIMO corrective and preventative maintenance work order system this Fall. Information about this finding will be shared with the MAXIMO project team to ensure that the security/roles are setup appropriately. City staff have been reconciling and reviewing the master inventory list to ensure accurate counts and conversion for the transition of inventory items to the MAXIMO system. Inventory management processes also will be developed for monitoring and auditing the City's inventory items in MAXIMO based upon already established inventory policies and procedures. Until the business function transitions to MAXIMO, we will implement separation of duties practices with these two staff and also monitor through audit queries within the system.

Finding 2: Administrative Access

We noted six shared administrative accounts to the COMET application and two each at the supporting Windows Server and Oracle database level. The six application level administrative accounts have passwords that do not expire until 2050 while the server and database level shared administrative accounts do not expire. A software tool named Password Safe was used to retain the shared administrative account passwords at the database and server level. Administrators login to the tool using a shared master account and password that creates a lack of accountability on who used the shared administrative account passwords retained within the tool. Thus, we would be unable to identify who and when a shared administrative account was used to perform administrative functions at the server and database level.

Administrative Access – Recommendation

Access to perform administrative functions should be limited to a small number of the IT support staff who use their individual accounts in order to maintain accountability. In certain instances, shared administrative accounts need to remain active in order to support on-going batch jobs and transfer of data between the application and database layers. The COBIT IT Framework policy guidelines recommends logging of who and when the shared administrative accounts are used, review the logs periodically and change the passwords to those shared administrative accounts periodically or when users with knowledge of those passwords leave the organization. A different form of password management should be considered in lieu of Password Safe as it doesn't provide for accountability of its use.

Administrative Access – Management Response

Passwords for all but two[1] of the administrative accounts referenced in the findings are managed in PasswordSafe. IT believes use of this solution to auto-generate and secure administrative and system service-account passwords is sufficiently secure, and represents a significant improvement over past practices. The encrypted database is located in a locked-down[2] folder on the M drive to which only six IT staff, including the team's manager, have access. IT acknowledges that this product does not support individual, named passwords for accessing the password manager. Because the password manager holds some passwords that the team needs to access multiple times per day, it isn't feasible to maintain a manual logging procedure. IT will research other solution options that support multiple named-user accounts or explore other ways to log access to the current solution.

Finding 3: Access Reviews

A user access review is a process that an organization implements to periodically check and verify the appropriateness of a users' access to systems and applications based on the user's job responsibilities. We noted that no formal access reviews were performed for the users and their assigned roles in the COMET application or its supporting servers and databases. This creates the potential risk of unauthorized access going undetected, which could result in invalid changes or loss of data.

Access Reviews – Recommendation

Implement an annual user access review that checks user privileges in order to note their on-going validity of access. The access review should be done for users at the application, operating system and database level. No user should review their own assigned access and any changes to access due to the review should be documented in order to maintain an audit trail.

Access Reviews – Management Response

The Minnesota State Auditor conducts an annual user access audit of financial system users by taking a sample of users to 1) review their user access documentation and approval, 2) confirm

[1] - These two are Oracle built-in accounts that are locked (not in use).

[2] - One must be logged on to the network with an active Windows domain account to access this folder.

that access was terminated for any employees who are no longer with the City of Minneapolis or have transferred jobs within the City and 3) confirm that users who have terminated their employment with the City did not access the system after their termination date. The functional support team for the financial system also reviews and confirms the list of City department staff who approve requisitions in COMET on a quarterly basis. Lastly, on a bi-weekly basis the functional support team reviews the list of terminated employees who have either left City employment or transferred to another position within the City to ensure that their system access is deactivated or updated for any current City staff who still have a business need to use COMET. The City has not engaged in a more comprehensive review of all system users (totaling approximately 725); although, the bi-weekly review process is a proxy method for checking and verifying the appropriateness of a users' access to systems and applications based on the user's job responsibilities. The City will implement a more thorough periodic review of all users to audit their system role and confirm the continued business need for that role assignment. This will require approximately 12 months to research, design and implement a process for this level of review. The City expects to engage a consultant to support this work effort with an estimated cost of $50,000.

Since 2012, Peoplesoft Systems have been the subject of several Internal and the annual State of Minnesota audits[3]. Each of these has involved a review of some or all of the contexts for user access, including IT administrative access, noted in the recommendation. Also during this time, the systems have undergone two major upgrades and migration to a new datacenter. Infrastructure and admin access accounts have been reviewed and updated, where appropriate, as part of all these activities. IT Security is currently conducting a baseline review of database and operating-system accounts for all systems migrated to the new datacenter. Going forward, IT Security will conduct periodic reviews of database and OS access accounts for Peoplesoft systems, and will participate with the Finance department to review Peoplesoft Financials application accounts for IT staff.

Finding 4: Secure Configuration & Change Management

A secure configuration standard is an internal standard implemented by a company in order to define minimum baseline configurations to help set a security standard for its IT assets. There are no defined baseline standards for the database and operating system supporting COMET and this creates a potential risk of a vulnerable system that may lead to unauthorized access or loss of data.

Patches containing fixes for known vulnerabilities or functional changes are published by vendors periodically. These patches should be evaluated to note the impact to the secure configurations defined and if they should be applied to the systems. We noted that there were no patches applied to the Oracle database in 2016 and there was no audit trail to note the rationale of leaving the databases unpatched. While the servers were patched in 2016, we were unable to obtain any documentation supporting the reason for application and if the patches were appropriately tested and approved before application.

Secure Configuration & Change Management – Recommendation

Implementation of secure configuration standard will minimize unauthorized access to the database and operating system as well as help in understanding any security vulnerabilities in

[3] - State of Minnesota audits of the Peoplesoft Financials system are performed annually.

the system setup. These baselines should be implemented and IT assets should be evaluated against the baseline periodically to note any system vulnerabilities. Any vulnerabilities noted should be reviewed for implementation and appropriate needed changes should be made in order to adhere to the standards defined.

In order to prevent the operating system and database levels of the system from being vulnerable to known threats, patches should be evaluated when released by a vendor and consequently applied if needed. Patch evaluation, testing and approval to move to production should be documented and retained in order to maintain auditability and tracking of patches applied.

Secure Configuration & Change Management – Management Response

Secure Configuration Standards

IT agrees that it is important to have secure configuration standards in place for IT infrastructure and applications. As noted in the management response to a previous Internal Audit, IT is in the process of defining and finalizing secure configuration standards for IT infrastructure (servers and database management systems) hosted with our new data center managed services provider, OneNeck. Similarly, procedures to monitor standards compliance as systems are built and released for use are being defined and finalized. Servers and database management systems are being built to these standards as they exist in draft form now. Similarly (as noted in a previous and recent audit response), IT has committed to perform a secure configuration review of the newly upgraded PeopleSoft applications.

Additionally, IT has contracted for services to perform regular Internal and External vulnerability scans of all systems that it is responsible for managing. Development of the regular scanning schedule and remediation process is underway.

Patch/Change Management

Windows Operating System Patches: IT has an undocumented, but consistently practiced, procedure for the Windows patching cycles. When Microsoft releases new patches (usually on the second Tuesday of the month), they are evaluated by IT and OneNeck to determine if any present significant risk and shouldn’t be applied. Within in two-days of release, the selected patches are installed in Test/Quality-Assurance environments. Application support teams are notified that these environments are ready for testing. If there are no issues reported, production patches are applied during the following Sunday maintenance window.

When production patching is complete, application support personnel is again notified. They are responsible to test and send email before end-of-day Sunday to acknowledge that their applications are back up and functioning properly. Note that it is extremely rare to encounter issues caused by the patches themselves, though there are occasional issues with the restart procedure after patches are installed.

There are SLAs built into the contract with OneNeck to measure and report on patch-installation success rates. This helps make sure that any issues with the installation procedure are discovered and remediated. The overall Windows patching procedure, including this confirmation step, will be documented in the City/OneNeck Procedures Manual when it is finalized later this year.

Oracle Patches: Oracle typically issues its critical security update (CPU) patches on a quarterly basis. IT acknowledges that patches released in the first two quarters of 2016 were not immediately applied to the Peoplesoft databases while the systems were being prepared for the upgrade. The upgraded system went live in late August. All 2016-released database patches have now been applied. The Oracle patching process is similar to the Windows patching process – undocumented, but consistently applied. The only difference is that the business owners may be asked to confirm testing prior to production install if the Peoplesoft support team believes that a patch could cause functional issues.

For all patch management activities, IT will focus efforts on its vulnerability management process to evaluate patch levels and document any business justification for patches that are not applied to systems.