County of San Diego

Auditor and Controller

OFFICE OF AUDITS & ADVISORY SERVICES

PEOPLESOFT HRMS APPLICATION AUDIT

FINAL REPORT

Chief of Audits: Juan R. Perez
Audit Manager: Lynne Prizzia, CISA, CRISC
Senior Auditor: Franco Lopez, CISA, CISSP, CIA, CPA

Report No. A17-018

August • 2017

Intentionally Left Blank

County of San Diego

TRACY M. SANDOVAL
DEPUTY CHIEF ADMINISTRATIVE OFFICER/
AUDITOR AND CONTROLLER

AUDITOR AND CONTROLLER
OFFICE OF AUDITS & ADVISORY SERVICES
5530 OVERLAND AVENUE, SUITE 330, SAN DIEGO, CA 92123-1261
Phone: (858) 495-5991

JUAN R. PEREZ
CHIEF OF AUDITS

August 14, 2017

TO: Susan Brazeau, Director
Department of Human Resources

FROM: Juan R. Perez
Chief of Audits

FINAL REPORT: PEOPLESOFT HRMS APPLICATION AUDIT

Enclosed is our report on the PeopleSoft HRMS Application Audit. We have reviewed your response to our recommendations and have attached it to the audit report.

The actions taken and/or planned, in general, are responsive to the recommendations in the report. As required under Board of Supervisors Policy B-44, we respectfully request that you provide quarterly status reports on the implementation progress of the recommendations. You or your designee will receive email notifications when these quarterly updates are due, and these notifications will continue until all actions have been implemented.

If you have any questions, please contact me at (858) 495-5661.

JUAN R. PEREZ
Chief of Audits

AUD:FL:nb

Enclosure

c: Tracy M. Sandoval, Deputy Chief Administrative Officer/Auditor and Controller
Damien Quinn, Group Finance Director, Finance and General Government Group

INTRODUCTION

Audit Objective

The Office of Audits & Advisory Services (OAAS) completed an audit of the PeopleSoft Human Resource Management System (PeopleSoft). The objective of the audit is to evaluate the adequacy and effectiveness of internal controls over PeopleSoft business processes.

Background

As the County's human resources information management system, PeopleSoft is the system of record for County employee and payroll information. County PeopleSoft users can be classified into one of two access types:

1. **Self-Service**: Self-service access allows users to view and update specific elements of their own personal, payroll, and benefit information. All County employees are granted self-service access to PeopleSoft upon hire.

2. **Privileged**: There are several tiers of privileged access which allow users to perform additional functions and/or have access to additional records. PeopleSoft administrators from the Workforce Information Network (WIN) Unit of the Department of Human Resources and DXC Technology (DXC) are granted the highest level of privileged access.

As of December 2016 there were 18,702 active profiles in PeopleSoft comprised of 753 accounts (4%) with privileged access and 17,949 accounts (96%) with only Self-Service access (See Appendix I).

Roles and permission lists provide the mechanisms by which access is restricted and separation-of-duties (SOD) is enforced in PeopleSoft. Access is granted to individual user or system profiles through the assignment of roles. Roles are comprised of multiple (predefined and customized) permission lists that are aligned to the business processes and functions to which a specific role requires access. As of December 2016, 840 roles were available for assignment in PeopleSoft, with 241 assigned to at least one active user.

The County's PeopleSoft security model has significantly matured since the previous audit (issued April 2010). Improvements made include:

- Password controls were updated to follow County standards
- Implementation of a security monitoring program
- Updated policies and business rules

Audit Scope & Limitations

The scope of the audit included a risk based assessment of the effectiveness of the County's current PeopleSoft HRMS Application business controls. Based on the assessment, the audit program focused on access and security business controls as outlined in the methodology. The review focused on the PeopleSoft system from December 2016 to April 2017.

This audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing prescribed by the Institute of Internal Auditors as required by California Government Code, Section 1236.

Methodology

OAAS performed the audit using the following methods:

- Interviewed stakeholders from DXC, Department of Human Resources (DHR) and the Auditor and Controllers (A&C).

- Assessed risks in select business processes within DHR and A&C.

- Reviewed PeopleSoft technical references, industry benchmarks, and best practices guidance.

- Reviewed County security standards and policies to understand organizational security requirements and guidelines, including the:
  - CoSD-T424 Security Management Plan (T424).
  - CoSD-T412 User Account Management Plan (T412).

- Assessed the usage and general design of roles and permission lists. This included assessing current PeopleSoft SOD rules and exceptions.

- Assessed the configuration and settings of high risk areas in PeopleSoft. This included review of user access lists.

- Assessed the effectiveness of the monitoring programs in place.

Audit Results

Summary

Within the scope of the audit, internal controls over the PeopleSoft application's business processes were generally effective. As outlined in the Audit Scope, OAAS' risk assessment led to an audit program focused on access and security business controls. Several opportunities for improvement in these areas were identified as outlined in the findings and related recommendations below.

Finding I: Privileged User Access Can be Further Strengthened

The majority of County user profiles (17,949) are assigned limited PeopleSoft access through the Self Service role; the remaining (753) profiles have varying levels of privileged access relative to their job duties. As such, privileged access within the application is assigned to only 4% of PeopleSoft users.

To assess business controls over these privileged users, access to sensitive pages, separation of duties design, and the WIN Units monitoring program were reviewed:

- **Access Review** – Access review of 26 sensitive PeopleSoft items (See Appendix II) identified that privileged users from DXC, the WIN Unit and (to a lesser degree) the A&C Central Payroll Administration (Payroll) are assigned complex overlapping roles embedded with multiple permission lists. This design allows for scalability, but also has the consequence of assigning these users broader access than needed for their job duties.

- **Separation of Duties Design** – The Security Role Matrix maintained by the WIN Unit outlines 30 roles that have defined conflicting relationships. After review with the WIN unit, no additional conflicts were identified within the remaining (211) active roles. However, review verified that conflicting relationships are allowed for PeopleSoft administrators in DXC, the WIN Unit and Payroll.

- **Monitoring Program –** The WIN Unit has a monitoring program in place that is designed to capture activity conducted by all privileged users for review. Testing concluded that the WIN Unit is effective at monitoring privileged user activity after its occurrence. No issues were noted.

Current SOD rules and least privilege configurations apply to all PeopleSoft users except for administrators within DXC, the WIN Unit and Payroll. While this has provided for generally effective business controls for over 99% of users, administrators are granted broader access than generally needed for their job duties. Limiting access to administrators (through SOD rules and least privilege configurations) would supplement current monitoring activities that ensure administrator activity within PeopleSoft is appropriate.

SOD's address the potential for abuse of authorized privileges and helps to reduce the risk of erroneous, inappropriate or unauthorized activity. The County employs the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.[1]

Recommendation: The WIN Unit, DXC, and Payroll should work together to identify and mitigate gaps in the current design of SOD rules and least privilege configurations. Related security documentation should be updated as necessary.

Finding II: Opportunities to Strengthen Administration Identified

Several opportunities were identified to strengthen administrative activities which help ensure business controls are operating effectively. Specifically, review identified:

[1] County of San Diego Administrative Manual 0400-03 Computer Accounts – Management and Use. For further guidance see the National Institute Standards and Technology (NIST) Special Publication (SP) 800-53 AC-5 & 6.

- Inconsistencies with system documentation.
- SOD exceptions to the Security Role Matrix.
- A monitoring program based on an informal risk assessment.

Inconsistencies with System Documentation – Review of documentation for roles and permission lists identified specific instances in need of maintenance and enhanced documentation. Additionally, examples of inconsistent application of the naming convention for permission lists were identified.

- PeopleSoft has 840 roles available, with 241 assigned to active users. Of those 241 roles assigned, 237 are descriptively outlined in the Security Role Matrix. The remaining 599 roles are comprised of prepackaged generic roles and customized roles created by administrators. All 840 roles represent access vectors into PeopleSoft and should have an adequate documentation trail. Having complete role and permission list documentation provides a standard for enforcement of appropriate logical access design.

- PeopleSoft Business Rules (PS-SC 1.3) outline a standard naming convention for permission lists designed to provide a general description of their purpose. However, not all permission lists follow the naming convention, making it difficult to assess the level of access these permission lists allow. Additionally, examples were identified where the permission list name did not follow the intent of its naming convention. Specifically, the following scenarios were identified:

    - Permission lists designed for transaction processing but also had correction access.

    - Permission lists designed for view only access but also had correction access.

SOD Exceptions to the Security Role Matrix – Review of the SOD Role Matrix against current active users identified 11 user profiles that have SOD conflicts. Discussion with the WIN Unit identified that these instances will likely be allowed exceptions to SOD rules and updated in the matrix.

Monitoring Program Can Be Improved – As previously noted, the monitoring program is effective at reviewing and following up on audit queries of system activity. These queries came into fruition over the life-cycle of the system as needs were identified. However, queries based on a formal risk assessment would ensure a more effective monitoring program which addresses high impact risks. Continuous monitoring programs should facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions as outlined in NIST SP 800-53: RA-3.

Recommendation: To further strengthen administration over PeopleSoft, the WIN Unit should:

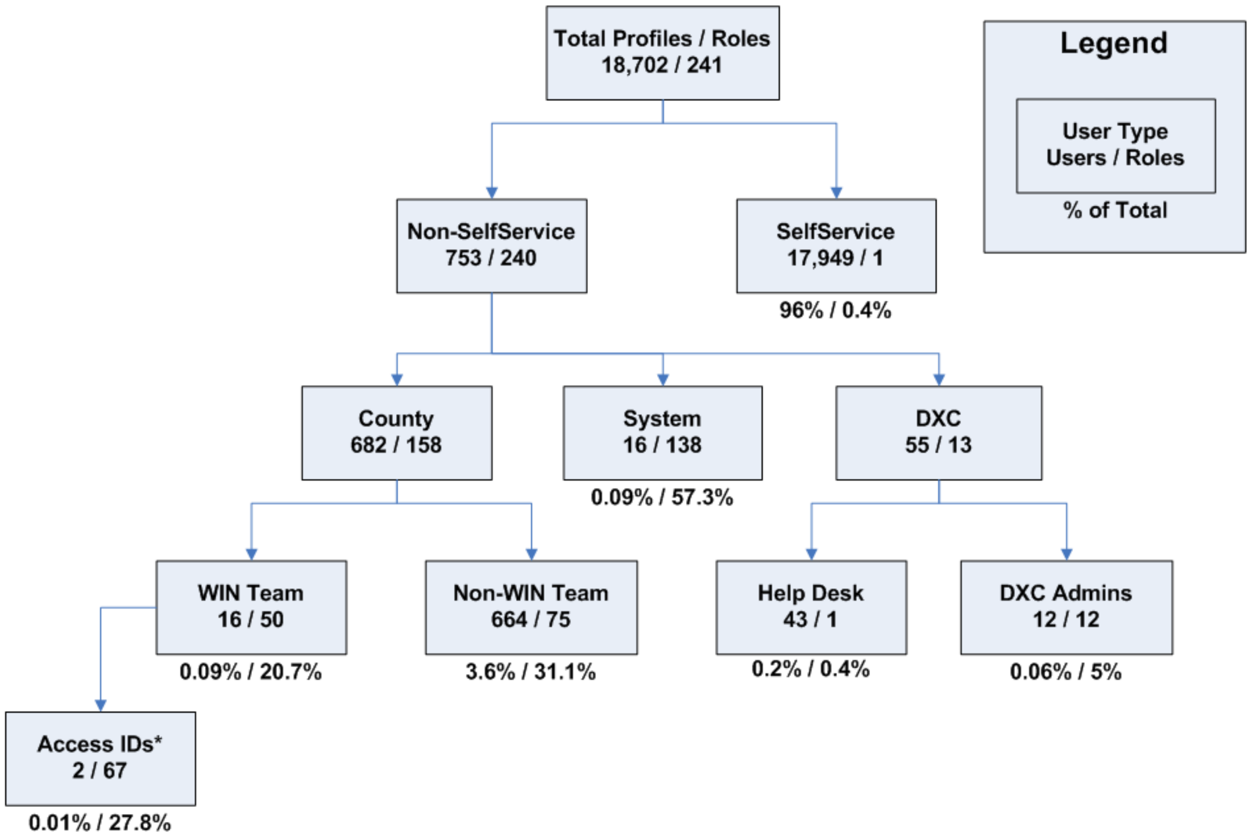
1. Update documentation for the creation and use of permission lists and roles to clearly outline generic roles from those used by the County.

2. Formalize a maintenance review plan for permission lists and roles to enhance the WIN Unit's review process.

3. Formalize a risk assessment program to monitor activities that may need updating due to process changes.

APPENDIX I

PeopleSoft Production Profile/Role Breakdown
December 2016



**Note: Access IDs are highly privileged profiles designed to allow select DHR employees to conduct tests that require broader access than allowed by their regular profile.*

APPENDIX II

26 Sampled PeopleSoft Items

1. Bar Item Name: Deduction_Table
2. Bar Item Name: Earnings_Table
3. Bar Item Name: Employee Garnishment Page
4. Bar Item Name: JOB_DATA
5. Bar Item Name: ONLINE_CHECK
6. Bar Item Name: Pay_Calculation
7. Bar Item Name: SD_RUNCNTL_INT028
8. Bar Item Name: SD_RET_EERT_TBL
9. Bar Item Name: SD_RET_ERRT_TBL
10. Menu Name: Application Engine
11. Menu Name: Cube Manager
12. Menu Name: Data Mover
13. Menu Name: DEFINE_PAYROLL_TAXES
14. Menu Name: EDI Manager
15. Menu Name: Maintain Security
16. Menu Name: Mass Change
17. Menu Name: Object Security
18. Menu Name: Process Scheduler
19. Menu Name: Row Level Security
20. Menu Name: Tree Manager
21. Menu Name: Utilities
22. Menu Name: Workflow Administrator
23. Object Group Security Settings
24. Role: PeopleSoft Administrator
25. Role: Process Scheduler Admin
26. Row Level Security Review

DEPARTMENT'S RESPONSE
(DEPARTMENT OF HUMAN RESOURCES)

County of San Diego

SUSAN BRAZEAU
DIRECTOR

DEPARTMENT OF HUMAN RESOURCES
EXECUTIVE OFFICE
1600 PACIFIC HIGHWAY, ROOM 203 SAN DIEGO, CA 92101-2463
(619) 531-5100 / FAX (619) 236-1353

TO: Juan R. Perez
Chief of Audits

FROM: Susan M. Brazeau, Director
Department of Human Resources

DEPARTMENT RESPONSE TO AUDIT RECOMMENDATIONS: PEOPLESOFT HRMS APPLICATION AUDIT

Finding I: Privileged User Access Can be Further Strengthened

OAAS Recommendation: The WIN Unit, DXC, and Payroll should work together to identify and mitigate gaps in the current design of SOD rules and least privilege configurations. Related security documentation should be updated as necessary.

Action Plan: DHR agrees with the OAAS Recommendation.

DHR worked with DXC in the spring to develop a module in PeopleSoft that formalizes the request and review of all user access requests for PeopleSoft. This module formalizes the request process, and tracks the request and its approvals or denial. This module will be rolled out in the first quarter of FY 2017-2018, and will further strengthen DHR's approach to the review and approval of access requests prior to their assignment. This will also assist in the monthly and/or quarterly auditing process to having details of changes to user accounts tracked in PeopleSoft. This work has been performed under SD-WR-026606 - SWE - Apps - PS - Custom Security Log page in PeopleSoft - implementation - VLR which began in January 2017.

Planned Completion Date: October 31, 2017

Contact Information for Implementation: Sandra Murillo (858) 505-6303

Finding II: Opportunities to Strengthen Administration Identified

OAAS Recommendation: To further strengthen administration over PeopleSoft, the WIN Unit should:

1. Update documentation for the creation and use of permission lists and roles to clearly outline generic roles from those used by the County.

2. Formalize a maintenance review plan for permission lists and roles to enhance the WIN Unit's review process.

3. Formalize a risk assessment program to monitor activities that may need updating due to process changes.

Action Plan: DHR agrees with the OAAS Recommendation.

1. DHR has updated the permission lists as identified during the audit in order to assess the level of access these permission lists allow. The permission list name now follows the intent of the naming convention. The two permission lists, one designed for transaction processing and one with view access only, had correction access due to system limitations. Those were included in the updates.

2. Current role assignments for privileged users are based on the access needed for the work that is conducted. WIN currently maintains what is technically a payroll table, but whose values are entered on employees' Job records. Central Payroll also accesses this table for entering and updating codes for the Additional Pay table, which is part of the payroll module. The table is crucial for the correct payment of pay components not reflected in the hourly rate used to calculate an employee's base salary. We will formalize regularly scheduled maintenance meetings with Central Payroll to review payroll roles that are assigned to privileged users.

3. DHR continuously monitors the higher level risk assessments conducted by the County's IT vendor. CTO requires that the security of Peoplesoft is evaluated by the security of our systems via our IT vendor. The Security Checklist is reviewed for compliance with County standards with every project, and remediated as soon as possible. Risk assessment and monitoring based on NIST SP 800-53 is a requirement of the IT Contract that went into effect July 1, 2017. According to CTO, processes and standards are currently being developed. Once the IT Contract processes and standards are finalized, DHR will update risk assessments and monitoring activities, if applicable.

Planned Completion Date: October 31, 2017

Contact Information for Implementation: Shelley Rieth (858) 505-6302

If you have any questions, please contact Elena Lepule at (858) 505-6375.

Susan Brazeau

Susan M. Brazeau
Director, Department of Human Resources

SB:sr