THE REGENTS OF THE UNIVERSITY OF CALIFORNIA
OFFICE OF ETHICS, COMPLIANCE AND AUDIT SERVICES

1111 Franklin Street, 5th Floor • Oakland, California 94607-5200 • (510) 987-0479 • FAX (510) 287-3334

Sheryl Vacca
SENIOR VICE PRESIDENT
CHIEF COMPLIANCE AND AUDIT OFFICER

May 26, 2016

DEPUTY CHIEF INFORMATION OFFICER CIANCA
EXECUTIVE DIRECTOR LEEDY

RE: Final Advisory Report Project No. P16A010: PeopleSoft HCM Segregation of Duties Review (Phase II)

Attached is a copy of the final report for Project No. P16A010: PeopleSoft HCM Segregation of Duties Review (Phase II). With the issuance of this final report, please destroy any previous draft versions. We very much appreciate the assistance provided to us by you and members of your staff during our review. If you should have any questions please feel free to contact me at 510-987-9646 (email: matthew.hicks@ucop.edu).

Matt Hicks
Systemwide Deputy Audit Officer

Attachment

cc: Senior Vice President Vacca
Program Manager Kolodziejski
Director Allison
Senior Manager Freire
Manager Cataldo
Contractor Uyboco
Consultant Kelly
Contractor Nash

UNIVERSITY OF CALIFORNIA
OFFICE OF THE PRESIDENT
INTERNAL AUDIT SERVICES

PEOPLESOFT HCM SEGREGATION OF DUTIES REVIEW (PHASE II)

Advisory Service Project No. P16A010

OCTOBER 2015

Work Performed by:
Martin Nash, Contractor
Harshita Bansal, Contractor

Executive Summary

Introduction

The University of California is currently undertaking a system-wide initiative to implement a single payroll, benefits, Human Resources (HR) and academic personnel solution for all UC employees. The technology that is being implemented as part of this initiative is the PeopleSoft Human Capital Management ("HCM") system. As a result of this initiative, UCPath, will:

- Replace the thirty-five year old Payroll/Personnel System (PPS) with a single new payroll and HR technology system
- Standardize and streamline payroll and HR processes system-wide
- Centralize certain HR and payroll transactional processes within the UCPath shared service center

As part of the University of California Office of the President (UCOP) 2014 – 2015 fiscal year internal audit plan, Internal Audit proposed to perform a Segregation of Duties (SoD) review of the implementation of PeopleSoft HCM at UCPath.

Objectives and Scope

The primary objective of the advisory service project was to identify potential SoD conflicts in the pre-production system of PeopleSoft HCM at UCPath so that they could be addressed prior to system go-live. The detailed objectives of Phase II were to:

- Evaluate the PeopleSoft HCM security configuration for sensitive access and segregation risks
- Verify users were assigned appropriate PeopleSoft roles as required
- Verify PeopleSoft roles were designed as defined by requirements
- Assess the role management process to determine if key risks were controlled
- Evaluate the PeopleSoft support structure to understand if responsibilities were appropriately outlined and key functions were adequately separated

The scope for Phase II included a review of the pre-production environment's security configuration within PeopleSoft HCM. The pre-production environment was defined as the instance where security was configured based on defined requirements prior to cutover.

As a part of this review, Internal Audit evaluated the application security for the following SoD rules:

HR SoD Rules	
Administer Workforce and Maintain Payroll	Manage Payroll Process and Plan Salaries
Administer Workforce and Maintain Payroll Interface	Maintain Payroll Interface and Plan Salaries
Administer Workforce and Administer Benefits	Role Employee and Role Manager
Administer Workforce and Define Payroll Tax	Role Employee and Capture Time and Expenses

HR SoD Rules	
Maintain Payroll and Manage Payroll Process	Manage Payroll Process and Administer Benefits
Maintain Payroll and Administer Interfaces	Configuration and Transactional Access
Administer Workforce and Manage Payroll Process	Manage Payroll Process and Role Employee
Manage Payroll Process and Define Payroll Tax	Administer Workforce, Maintain Payroll, and Manage Payroll Process
Manage Payroll Process and Define Time Labor	Administer Workforce, Maintain Payroll, and Plan Salaries

Procedures Performed

To accomplish the project objectives, Internal Audit performed the following procedures for Phase II:

1. Held a kickoff meeting with key IT and process owners / personnel
2. Received and reviewed the following process documents and data:
    a. Data extraction of key PeopleSoft HCM security tables from pre-production instance of HCM
    b. User Mapping Matrix
    c. Role Design Matrix
3. Evaluated PeopleSoft HCM security configuration for key risks
    a. SoD risks using the Assure tool (Protiviti proprietary tool used to evaluate application security risks)
    b. Role / Permission List design risks (determine if roles / permission lists were configured consistent with requirements)
    c. Excessive access risks (determine if users were provided additional roles beyond what is required)
4. Reviewed future state HRIS support and maintenance process documentation
5. Held meetings and workshops with Client's IT team to review and validate findings
6. Provided potential remediation recommendations to Client's IT team
7. Received management responses and action plans

Deliverables

Deliverables for Phase II of this advisory service project include a document summarizing the key SoD observations, detailed User ID comparison results and a detailed Role design comparison document. Refer to the following deliverables:

- UCPath Role Design Analysis - Final.xlsx
- UCPath User Role Validation -Results-Final.xlsx
- Base Roles for Each User Group.xlsx
- UCPath PSFT HCM SOD Risk Analysis - UC Responses_Detailed Summary.xlsx

Key Observations and Management Actions

Below is a summarized list of key observations identified based on the work performed during Phase II. Refer to the Deliverables section for workpapers and detailed observations.

1. Segregation of Duty Risks

Internal Audit identified user accounts with access to conflicting functions based on the segregation of duty risks outlined above. While most of the user accounts identified will not be part of the production environment (following go-live), two (2) user accounts will have access to maintain payroll data and manage the payroll process. This is an increased risk to the organization as users with this access have the ability to enter fictitious or unauthorized payroll information including: setting up direct deposit, defining additional pay earnings, and defining tax data, to an employee and processing the unwarranted request allowing the employee to receive inappropriate wages or earnings. Additionally, Oracle On-Demand (OOD) support accounts, which are used to maintain the system, appear to have pervasive access, thus creating significant segregation of duty risks.

UCPath Center (UCPC) HRIS, who is responsible for security administration to HCM, will implement procedures to proactively identify potential segregation of duty risks during the provisioning process. Internal Audit recommends performing a quick assessment following the go-live to verify: 1) all testing and implementation of user accounts has been removed and 2) segregation of duty checks are operating effectively. Additionally, we recommend implementing a level of monitoring on the OOD user accounts to help mitigate the risk of inappropriate transactions from being entered into the system.

Action Plan:

User accounts with conflicting functions: Due to the limited number of payroll resources, there needs to be some cross over in access. UCPC Production will run audit reports to capture and monitor data changes in direct deposit, pay sheets, pay for UCPC staff, and balances adjustments. Once UCPC initiates the staffing for the Pilot, UCPC IT HRIS will modify access to limit the staff ability as described following UCPC management approval.

Target date: 08/31/16 (It is expected that payroll will have hired and trained staff to segregate duties.)

OOD support accounts with pervasive access: This will require an update on the need for this level of access from Oracle. UCPath PMO technical team lead received the following information from Oracle regarding each Oracle on Demand account:

- Our Oracle On Demand (OMCS) user OOD_ADM has always had full access to a customer's environment. It's pretty much a clone of PS or VP1 and we also clone permission lists and roles that were delivered out of the box. This clone process is part of application hardening process that has been in place for years since Oracle started hosting customer environments in On Demand. Only those that support our PeopleSoft customers have access to OMP in which we store IDs and passwords for our supported accounts. There is also an algorithm put in place to change this password. Please understand that ALL of our customers have this user account in their environments. It's also used for troubleshooting purposes when issues come about.

- OOD_IB – used only for integration broker setup. Created as clone of OOD_ADM.
- OOD_OMCS_TEST – not in use, can be deleted.
- OOD_PSAPPS – Used to configure for APP, Process scheduler startup/shutdown, report distribution.
- OOD_SES – used for SES configuration.
- OOD_XML – used for XML in web profiles.
- OOD_SKMHOSSAIN & OOD_SVANGA – created by UCOP for individual OMCS team members to access UCPath URLs. (These have very limited access).

Procedures to proactively identify segregation of duty risks: UCPC IT HRIS reviews security request forms and ensures no SOD conflicts prior to provisioning per documentation.

Target date: Completed

Procedures to monitor Oracle On Demand accounts: UCOP ITS will review the access levels and ensure they are appropriate. UCOP ITS will develop a query or report to look for transactions/tasks performed by OOD accounts.

Target date: 8/1/16 (30 days following availability of query or report used for monitoring activities of the Oracle On Demand accounts.)

2. HRIS Responsibilities Create Potential Segregation of Duty Risks

Based on the HRIS team's structure and responsibilities as per the "UCPath Center IT HRIS Team responsibilities and PeopleSoft Access" document, it appears the group will have a significant amount of responsibility and access to PeopleSoft HCM. In most organizations, the HRIS group is not responsible for performing security administration functions, as those are performed in the IT Security group. Based on discussions with UCPC, we understand the plan is to hire an analyst to allow separation of security responsibilities from other maintenance and support functions. Until this person is hired, Internal Audit recommends performing additional procedures to detect if inappropriate actions are occurring (e.g., changes to roles / permission lists, core and high risk configuration, key transactions, etc.). Additionally, UCPC HRIS will implement procedures to log and monitor key data changes within HCM. While this will help mitigate the risk, UCPC Management should have a formally documented process that provides information regarding who is accountable and responsible for logging and monitoring activities; including escalation procedures should issues be identified.

Action Plan:

Key Note: UCPC IT HRIS only performs configuration changes following the existing change request review and approval process through JIRA that requires UCOP, UCPC, and UCPath PMO leadership approval. Additionally, a Service Now request is required following the change request approval as well as UCOP ITS analysis prior to any configuration changes being implemented in the production environment.

UCPC IT HRIS only grants or changes access to UCPath based on Service Now requests with management approval.

Segregation of duties risk within the UCPC IT HRIS team: Due to limited UCPC IT HRIS staff, the existing HRIS Analysts are required to provide support, manage configuration/table updates, and administer application security. Until a security administrator is hired, the two Senior HRIS Analysts will be the only staff to create new or modify existing roles and permission lists. UCPC will hire a security administrator and transition responsibilities.

Target date: 12/1/16

Process for monitoring key activities performed by the UCPC IT HRIS team: Develop and document the process for monitoring activities related to role/permission list changes, and high risk configuration changes as well as the escalation procedures. This is in addition to the upfront review and approval process outlined under the key note above.

Target date: 6/1/16

3. PeopleSoft Roles Not Configured as Designed

Internal Audit sampled ten (10) roles from the PeopleSoft HCM pre-production environment to determine if they had been configured as defined by the requirements. All ten (10) roles were found to have additional page access that was not included in the design requirements. The additional page access allowed users to access critical administer workforce and payroll functions. UCPC Management is in the process of reviewing the findings and developing action plans / responses where applicable. Internal Audit recommends verifying all roles are designed based on business requirements to follow the rule of least privilege. This can be done through detailed testing or analytics on the access entitlements. Refer to the deliverable 'UC Path Role Design Analysis - Final.xlsx' for more information.

Action Plan:

Key Note: Once UCOP went live and users started to perform their duties, roles and permissions had to be adjusted because certain pages and actions were not available and are necessary to do their job. Some roles have also been modified to restrict some access once it was determined certain levels of access were not needed. Roles and permissions will continue to be refined as needed to support daily operations.

Verify roles for UCOP and UCPC users are appropriate: UCOP and UCPC management to confirm access is appropriate by leveraging the existing user to role mapping matrix.

Target date: 8/1/16 (dependent on availability of a report or query to be used for validation)

4. User Mapping Matrix is Incomplete

Internal Audit identified users that were assigned additional roles beyond what had been defined within the 'User Mapping Matrix', which was provided by the PeopleSoft project team and contains information regarding what roles are being assigned to users. Based on Internal Audit's conversation with the Functional Support Consultant, we verified that each user group had been assigned a specific set of base roles along with their functional role. We recommend updating the

'User Mapping Matrix' to reflect the security requirements for UCPath, even if all users require access to specific roles.

Action Plan:

The user to role mapping matrix is up to date for UCOP.

Target date: Complete