Port of Seattle®

PeopleSoft Upgrade Post-Implementation Audit

June 2015

Powerful Insights.
Proven Delivery.®

protiviti®
Risk & Business Consulting.
Internal Audit.

Table of Contents

Executive Summary

Objective

Protiviti was engaged by the Port of Seattle ("the Port") to perform a post-implementation review of the PeopleSoft Financials system upgrade from version 8.4 to 9.1 to determine if the upgrade achieved the overall implementation goals, if the functional performance and outcomes met the expected performance, to identify any lessons learned and to develop action plans, if necessary. This document summarizes the objectives, key observations, and recommendations resulting from these efforts as of April 2015.

Scope

The Post Implementation Review performed by Protiviti focused on the following key areas:

A. Business Case and Planning;
B. Change Management and Installation;
C. Risk and Risk Mitigation; and
D. Stakeholder Acceptance and Satisfaction
    i. Quality Assurance, Stakeholder Approvals and Benefit realization
    ii. PeopleSoft Current State Security Model Review

Approach

Protiviti adopted the following approach for the Post Implementation Review:

- Obtain and Review available documentation around the scope areas.
- Conduct interviews & demonstrations with stakeholders to understand processes, tools & repositories used during the implementation that were deemed relevant to the review.
- Data sampling to corroborate the understanding obtained via interviews.
- (For Security review only) – Assess current state of PeopleSoft security model in Production and validate observations with stakeholders.

Executive Summary

Highlights and Accomplishments

In the course of conducting this audit, several areas of strengths were observed that could be leveraged during future initiatives. The following is a list of highlights and accomplishments that the Protiviti team would like to note for the benefit of the Port's Management:

- **Delivery on project objectives and business functionality –** It was noted, via interviews with project team, stakeholders and Senior Management, that the project team successfully delivered on the key objectives and business functionality.
- **Project team collaboration –** Per inquiry with project team and stakeholders, it was observed that there was very close collaboration between Information Technology, Accounting and Consultant teams during the course of implementation. This was key to completing an implementing such a scale of implementation under budget without significant schedule extension.
- **Project budget planning and monitoring –** Planned budget and actual spend were closely aligned for this project, with the project being implemented under budget. Per inquiry, it was noted that budget was closely monitored, regularly updated and shared with Senior Management. There were contingencies built into the budget given the lead time required to obtain approvals prior to commencing a project and although these were not used, it indicates a good level of planning on the team's part to plan for unforeseen expenditure.
- **Risk management: Proactive Senior Management engagement and direction –** Per inquiry it was noted that the frequency of meetings with Senior Management increased as the project moved closer to implementation. Proactive engagement by Senior Management around risks was noted in the specific instance of resource changes implemented by the team as a result of "sit-down" meeting with the Consultant when a skill mismatch was observed. Also, following the direction laid down by Senior Management, the project team took some key decisions early on in the project (excluding Project costing and adopting as much as out-of-box functionality as possible) that reduced risk exposure and contributed to a successful implementation.
- **Planning documentation –** Review of project documentation and information gathered via interviews indicate a high level of initial planning, with detailed plans (Change Management Plan – for organization and system changes, Risk Management Plan and Project Management Plan) being created upfront.

Summary of Observations

PeopleSoft Security Review: Administrative Access All five members of Production Support team retain administrative privileges to the application environment and access to the database. Lack of traceability when logging into the Database using an administrative ID is a known issue in PeopleSoft (with MS-SQL) that leaves the database vulnerable to unauthorized changes that cannot be attributed to individual users.	**Risk:** High

Recommendation:

This level of access to financially sensitive information in the production environment is a high risk. Port Management or Internal Audit (IA) could potentially decide to lower the risk rating based on their assessment of the effectiveness of the business process controls put in place, both in terms of comprehensiveness of design and implementation effectiveness. Management should evaluate the below recommendations in the light of resource/staff availability and any existing contractual obligations:

- Investigate the possibility of an automated mechanism to actively monitor Production environment for unauthorized changes.
- Consider setting up a production-like environment for troubleshooting production issues.
- Consider implementing a secured password vault for storing Administrator password, access to which should be limited to the appropriate personnel, after obtaining the required approvals. Password should be changed after each access.
- Barring any changes to administrative access to reduce the risks associated with this observation, Port Management or Internal Audit should consider conducting a thorough review of business process controls for comprehensiveness of design and implementation effectiveness to evaluate if they adequately mitigate risks related to potential fraudulent activities.
- Consider assigning specific maintenance window for applying vendor-provided patches.
- Consider renegotiating SLAs with business, if required, in order to set expectations on turnaround time for resolving issue.

Management Response:

We disagree that this is a high risk issue. Shared administrative access due to deficiencies in Peoplesoft with a Microsoft SQL Server backend was a known issue and was openly discussed with Protiviti at the front end of the project performance assessment. The process controls from AFR detailed in item #2 provide additional layer of security to help mitigate this exposure. This exposure was also previously reviewed with Moss-Adams during our annual financial audit and was not considered to be a finding in their report.

As stated, this access has been strictly limited to 5 key PeopleSoft system administrators who pass FAA and Police background checks and who are essential to the operation and maintenance of our financials environment. To our knowledge no other user of this system has been successful in developing practical formal procedures to further mitigate this risk without impacting the operations of the system, or our ability to rapidly restore it in the event of an outage

Summary of Observations

PeopleSoft Security Review: Segregation of Duties (SoD) There is a lack of clear definition of roles or SoD in PeopleSoft resulting in some employees having excessive access and ability to perform potentially fraudulent transactions.	**Risk:** Medium

Recommendation:

Management should consider undertaking a full review of SoD and sensitive access followed by associated remediation measures. A comprehensive role definition should be created for PeopleSoft financials application with clear SoD. All roles providing duplication of access privileges should be appropriately remediated and roles that are not actively used should be removed from the database. Management should also establish a schedule for a review of role definitions and configuration (in Production environment) on a quarterly basis. Additionally, Management should also enhance the authorization request form to include accurate and detailed description of roles to ensure appropriate access is requested for staff.

Summary of Observations

PeopleSoft Security Review: Segregation of Duties (continued)	**Risk:** Medium

Management Response:

Port management appreciates Protiviti's observations resulting from their review of controls limited to IT systems risk, and respects that Protiviti could not independently verify the comprehensiveness of design or validate implementation effectiveness of the Port's augmenting business process controls in place, due to scope limitation of the audit engagement. Port management values Protiviti's recommendations and will give them serious consideration as we continue to seek opportunities to refine and improve the broader systems/process internal controls environment.

An important point is that in addition to the system access/roles security protocols in place that enable a user to transact in PeopleSoft Financials, the Port/Accounting & Financial Reporting (AFR) department has in place solid internal controls, as shared with Protiviti, in the form of fully documented business process internal controls. This combined internal controls framework is robust and is expected to addresses both financial systems risk and business process operational controls taken as a whole. Together, possible system risks are expected to be effectively mitigated through business process controls, as a key risk exposure to the Port involving its financial systems are the execution of fraudulent transactions that may result in a loss of funds or assets, or a material misstatement in its financial statements. Internal controls over all key transactional and business processes are in place.

The Port's overall system of internal controls (addressing both systems risk and financial business process risks) is audited annually by the Port's independent Certified Public Accounting firm (Moss Adams) as to design and operational effectiveness, as part of their audit of the Port's financial statements and federal awarded funds administration/regulatory compliance. These internal controls are also audited annually by the Washington State Auditor's Office as part of their public funds/assets accountability audit, focused on evaluating whether public resources are handled properly and in compliance with laws and regulations, and whether effective internal controls are in place to promote accountability and encourage sound financial management practices. The Port annually receives clean audits (no major findings) as to the overall design and operational effectiveness of the internal controls in place including the use of the PeopleSoft Financials system.

Summary of Observations

PeopleSoft Security Review: Segregation of Duties (continued)	**Risk:** Medium

Management Response: (continued)

The Port of Seattle acknowledges that a security design document for v9.1 setup/configuration is not currently present. Where a functional/technical design document may often be developed during a comprehensive upgrade project when security is configured; the PeopleSoft Financials v9.1 upgrade was a technical only upgrade and within this scope the Port did not utilize resources to fully implement formal best practice. Rather, the decision was to focus resources on functionality critical to business operations. It was decided that security would be rolled over to the new version status quo thus, a comprehensive design document was not completed at that time.

However, the Port does absolutely adhere to formal security administration protocols. While undocumented in terms of design, the business processes that support this key responsibility are firmly established and followed. All PeopleSoft Financials security requests go through a 3-tier review and approval process. First, requests are submitted to the respective operational workgroup manager for first tier approval. They are then forwarded to a separate team, the AFR Business Technology Analysts, for review/approval. They are then submitted to yet another separate group, the ICT PeopleSoft Developer team. The AFR Business Technology team does not have access to the PeopleSoft PeopleTools module where security access is administered. The ICT PeopleSoft Developers separately have this security access to update the end users security profile in PeopleSoft. Furthermore, a quarterly security audit, separately administered by the AFR Business Technology team, is also performed where each employee that has access to their PeopleSoft Financials module is reviewed by the workgroup managers for reasonableness and appropriateness.

The Port of Seattle appreciates and will consider the recommendation of creating a comprehensive security design document to document the security protocols in place and make any further refinements as informed through this audit.

Summary of Observations

PeopleSoft Security Review: Segregation of Duties (continued)	**Risk:** Medium

Management Response: (continued)

The Port of Seattle PeopleSoft Team (includes ICT PeopleSoft Developers and AFR Business Technology Analysts) partner, and share distinct and separate responsibilities, to administer security for PeopleSoft Financials. The AFR Business Technology team is responsible for approving and auditing all transactional add/update access to PSFS modules. The ICT PeopleSoft Developers are responsible for approving and auditing the delivered roles that are used by ICT to administer the database and associated tasks. For this reason, the Roles that the AFR Business Technology Analysts are responsible for are "hard coded" into the query criteria that is used to perform the audit. The role that this audit report references was an old, outdated, PeopleSoft delivered role that is no longer being used by AFR. Hence, it was not "hard coded" into the query criteria and, therefore, did not appear in the comprehensive quarterly audit review process.

We note that while there were roles identified that were not present on the PeopleSoft Financials Security Request Form, the administration and audit that is performed on our security module is very comprehensive and there are no employee's with inappropriate or unauthorized access. This is affirmed by AFR's quarterly review.

We have, however, recognized the opportunity presented and are developing new reports that will capture all roles that are assigned to any Port of Seattle employee, regardless of departmental ownership. The PeopleSoft Authorization Form will be updated to include all roles that are active in the Production environment.

protiviti

Summary of Observations

PeopleSoft Security Review: Segregation of Duties (continued)	**Risk:** Medium

Management Response: (continued)

The PeopleSoft Financials v9.1 Authorization Request form includes three (3) columns: the PSFS Module, Role, and Description. This form is completed by the end user, or end user's manager. The descriptions of the roles are intended to be generic as our audience is not necessarily of technical background. While the title may not be all encompassing, the information contained is accurate. The typical business process that is followed for security is for the end user to request that we "clone" another user who is performing the same work. The end user then populates the appropriate roles on the form to submit for approval. A form referencing the role description as the specific technical verbiage for the page/component name would cause confusion for our end users. Nevertheless, as we plan to develop a comprehensive security design document, we seek to find a practical balance of understanding for our end users. A permission list/page/component/add/update/correct description can be noted, in addition to a description that makes sense to the end user.

The above discusses the comprehensive system/roles security and transactional/operational internal controls in place. We also clarify that a different system security risk area that these controls would in part mitigate is in regard to Protiviti's observations provided under the section, "PeopleSoft Security Review: Administrative Access" which is responded to separately in that section.

Port management appreciates the analysis and observations noted by Protiviti. We will continue to build upon our sound internal controls that are in place, with serious consideration to the recommendations provided.

As we have collectively acknowledged, the technical upgrade from v 8.4 to v9.1 was in itself a massive and complex undertaking, but a very successful implementation that went live smoothly and which the Port is very proud of.