

PeopleSoft HCM Security Project

Version: 1.1

Date: 12/10/2005

Prepared by: Jeff Guhin

TS 5004 – Technical Communications
Final Project

Abstract

XYZ Company currently has multiple legacy systems used in production for Human Resources and Payroll applications. These systems are not fully integrated with each other which results in duplicate records, inconsistent naming conventions, and intensive manual corrections.

An Enterprise Resource Planning (ERP), package has been purchased from PeopleSoft. ERP is a business management system that integrates core business processes including planning, sales, marketing, order tracking, customer service, finance and human resources. The ERP system will be implemented one module at a time. The first module titled Human Capital Management (HCM), will launch December 18, 2005.

The PeopleSoft HCM application will help HR meet organizational objectives:

- Enable HR to serve the organization more strategically
- Improve service to employees and managers
- Reduce Administrative costs
- Eliminate process steps, approvals, and paper-based forms
- Increase employee satisfaction
- Enable manager access to data for improved decision making
- Increase information access
- Implement “best practice” process out of the box

The PeopleSoft ERP solution should have stringent security measures to prevent unauthorized end users from abusing their roles within the application. PeopleSoft defines security by providing access to data and tools users’ need to do their job (Oracle, 2005). Business Analysts determine who gets access to the application data and XYZ Company defines the network and database security model.

This document contains a compilation of three reports related to security. The Technical Overview, the Test Strategy and the Test Plan. The initial proposal can be referenced in appendix A.

Table of Contents

Technical Overview	3
Permission Lists, Roles, and User Profiles	4
Test Strategy	5
Purpose.....	5
Introduction.....	5
Schedule.....	6
Approach.....	6
Test Plan	7
Introduction.....	7
Project Quality Assurance Overview.....	7
Functional Specifications.....	8
Test Approach.....	8
Project Resources.....	9
Entrance/Exit Criteria	10
Types of Testing to be Utilized.....	11
Test Case Table.....	11
Required Test Environments.....	13
Defect Tracking	13
Scheduled Deliverables.....	14
Approvals	14
Revision History.....	15
Appendix A.....	15
References.....	18

Technical Overview

Access and manipulation of data need to be carefully controlled and tested. An employee entering Learner records should not have the permission to view employee payroll data. In the Human Resources solution of an ERP system an employee should not have the rights to approve his/her own performance appraisal.

Types of security testing should include: Security Design, User Profile Setup, Role & Permission List Setup, Process Security, Query Security, Row Level Security (for HR and Financials), Portal Security, Security Migrations, Definition Security, LDAP Authentication, Password Controls, and Dynamic Role Creation.

As with any core business application, security is critical to PeopleSoft ERP. Every department should not be allowed access to all the functions or all the data of all the applications. Access to PeopleTools should also be restricted to only those responsible for managing customizations of the application.

PeopleSoft provides security features to ensure that sensitive application data is adequately secured. This layer works on top of other security tools in place for the network and the Relational Database Management Software (RDBMS). All these components work together to create an infrastructure that protects the PeopleSoft system from unauthorized access.

As the PeopleSoft Internet Architecture (PIA) is implemented, a scaleable means is needed by which authorization to users can be granted efficiently. The PIA is presented below in figure 1. (Oracle, 2005). As XYZ Company continues to grow, the number of potential users of the system increases exponentially.

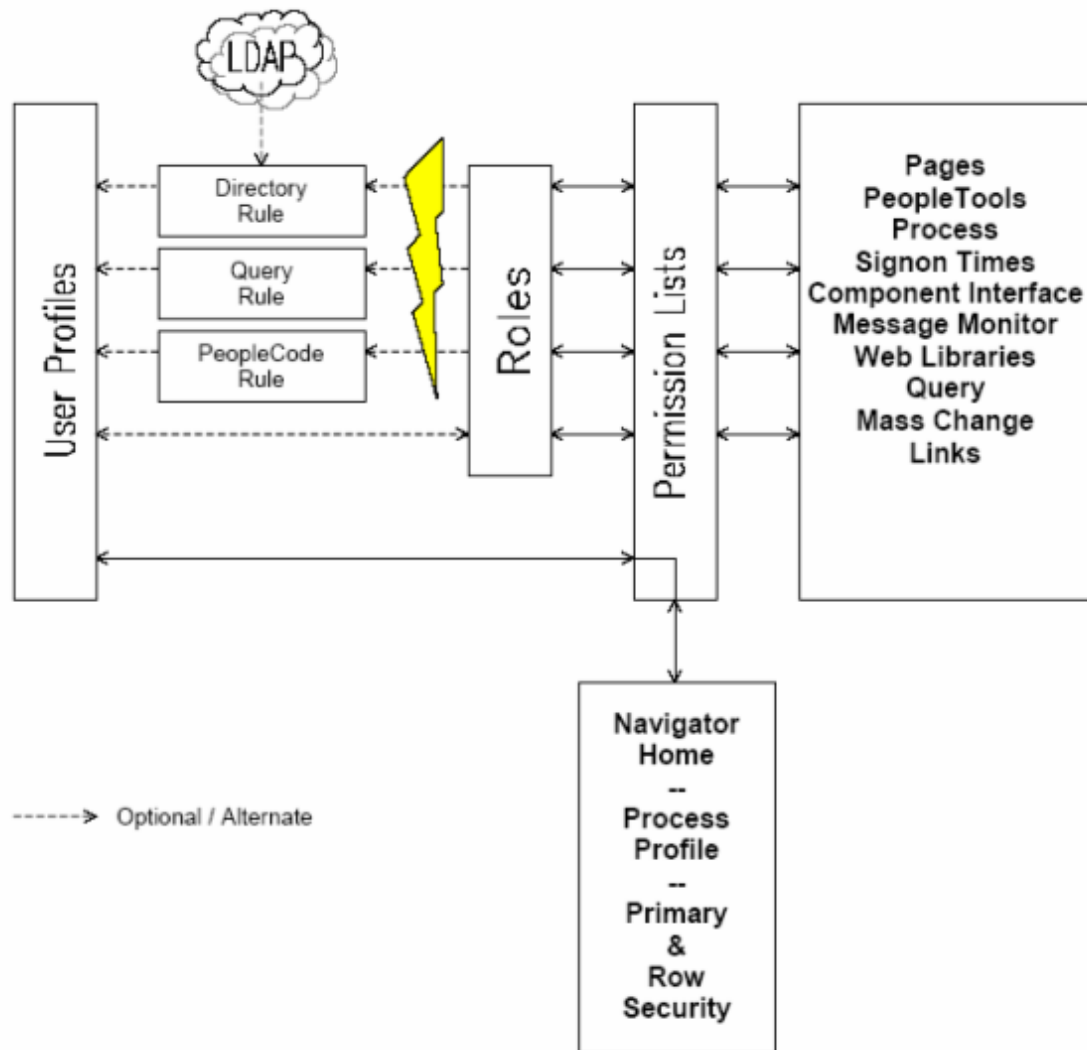


Figure 1. PeopleSoft Online Security Framework

Permission Lists, Roles, and User Profiles

The PeopleSoft security approach is designed for the Internet. Security definitions are easily created and maintained. Maintenance can be simplified through dynamic and automated processes programmatically.

Users can include registrars, applicants, learners, and so on, and can be grouped according to roles. Roles are security objects associated with information such as name, description, or permission lists. One of the properties attached to a role is the list of users assigned to it. For instance, there might be an Applicant role, a Learner role, or a Registrar role. Users who belong to a specific role require a particular set of authorizations and privileges within the system so that they can complete their daily tasks.

In addition to applying security authorizations to users, objects and definitions in the PeopleSoft development environment need to be protected from unauthorized access that could compromise the integrity of the system (Carter, 2005). Similar to access restrictions to pages and components, restrictions to the objects definitions that developers can access using Application Designer are needed.

Test Strategy

Purpose

The scope of this section relates directly to the roles and permissions associated to the user profiles in PeopleSoft system. For other areas, such as databases, file servers, or networks, appropriate strategies to secure and protect these components must be formulated separately.

Introduction

The PeopleSoft ERP solution should have stringent security measures to prevent unauthorized end users from abusing their roles within the application. PeopleSoft defines security by providing access to data and tools users need to do their job. Business Analysts determine who gets access to the application data based on approval from business or process owner and XYZ Company IT defines the network and database security model.

Access and manipulation of data need to be carefully controlled and tested. An employee entering time reporting should not have the permission to view employee payroll data.

For this project, the following apply to Security Testing:

Environment Information -- testing will occur in:

- A) DEV
- B) PROD

Test Coverage -- Test coverage will consist of the following:

- A) Test Types: Positive and Negative testing
- B) Applications/Modules Under Test: HCM
- C) Portal Links in Stella to HCM

In Scope

- LDAP authentication – phase 1
- IT Roles and permissions
- HR Roles and permissions
- Payroll Roles and permissions
- Employee Roles and Permissions
- Manager Roles and Permissions
- Query access manager

Out of Scope

- SSO

- PDI
- Auditing (record, field, database level)
- Dynamic role creation
- Personalization's
- Row level security
- Process security

Schedule

TASK	SCHEDULED START DATE	SCHEDULED DELIVERY DATE
Write Test Cases for functional roles & LDAP	11/28/05	12/09/05
Write Test Cases for IT roles	12/08/05	12/12/05
Code Freeze in DEV		12/12/05 9am
Security Testing in DEV	12/12/05 9am	12/15/05 5pm
Security Testing in PROD	12/16/05 3pm	12/17/05 5pm

Approach

Some IT/HR/Payroll profiles may have multiple business roles assigned. Roles will be tested based on how they are assigned to the user profiles. Critical tasks required for users to perform their jobs will be identified and mapped to the user profiles if they are assigned multiple roles. Positive testing will verify the users have access to the pages and functions they need. Negative testing will verify that users do not have access to IT/HR/Payroll data that is not required for their job.

A. Risks

- Defined requirements have not been documented for HR/Payroll business roles. QA is working with the functional BAs to determine testable security requirements for HR, Payroll, Time and Labor, and Employee/Manager self service.
- Defined requirements have not been documented for IT business roles and there is not a BA assigned to this task. The testable scenarios will be based on QA's interaction with the IT teams and the technical architect.
- Defined requirements have not been documented for LDAP. QA will test this based on the suggestions provided by the PeopleSoft consultant.
- The window for QA to test security in the production environment is limited to 12/16/05 at 3pm until 12/17/05. This is a short window to adequately test security and fix any potential defects.

B. Assumptions

QA will use actual user profiles in DEV. QA will use cloned user profiles in PROD.

Test Plan

Introduction

The purpose of the Introduction is to provide a high-level view of the contents of the Test Plan.

Systems Under Test

This Test Plan describes the steps that will be taken by the QA staff to test changes affecting the following systems:

- New Frontier – Human Resources and Payroll system

Document Contents

This test plan contains the following information:

- Project Description
- Any revisions to scope, risks, issues, or assumptions
- Business requirements and functional specifications to be tested
- Test Approach under this test plan:
 - Project Resources
 - Entrance and Exit Criteria
 - Test type
 - Test Cases
 - Test Environment(s)
 - Defect Tracking

Source Documents

This Test Plan is based on the following completed deliverables:

- Conceptual Solutions Document
- Security Test Strategy

Project Quality Assurance Overview

Project Description

XYZ Company is in the process of implementing PeopleSoft Enterprise applications. This phase relates to the implementation of Security in the Human Capital Management (HCM) module.

Changes to Scope

Requirements still need to be determined for the Record Level Auditing included in the December release of HCM .

Changes to Risk

1. If any issues are found during security testing, there may not be enough time to fix the issues and retest during the test window.

Mitigation Strategy: Get as much tested as soon as possible to find any errors as soon as possible.

2. Requirements for the roles and permissions assigned to user profiles have been changing daily as the project progresses. Documentation of the requirements may be incomplete.

Mitigation Strategy: Documentation of the changes being made are updated in TestDirector.

Changes to Assumptions

1. There will not be enough testing time to complete all of the security test scenarios.
2. Execution the ben admin process will be validated the HR users.
3. It is assumed that the PeopleSoft systems basic functionality works as expected. Testing will focus more on validating user profiles contain the appropriate business roles to perform their jobs.
4. Requirements for Record Level Auditing will be provided by the Technical Architect prior to testing in Development.

Functional Specifications

This section lists all business and technical requirements and indicates if they are in scope for testing under this test plan. For items listed as out of scope, information concerning their validation is provided.

In Scope Functional Specifications

Defined requirements were not available prior to starting the Test Strategy and Plan. All of the security specifications for the implementation of HCM were gathered from miscellaneous documents and conversations with the BAs, Technical Architects, and PeopleSoft consultants.

- PeopleSoft IT Roles
- PeopleSoft HR Roles
- Portal Uses Cases
- LDAP Integration
- Auditing (record level)

Out of Scope Functional Specifications

The following list of items will not be implemented in the December release of HCM.

- SSO
- PDI
- Dynamic role creation
- Personalization's
- Row level security
- Process security

Test Approach

The test approach describes the approach that will be used to validate the requirements and specifications that are part of the test scope. Some profiles may have multiple business roles assigned. Roles will be tested based on how they are assigned to the user profiles. Critical tasks required for users to perform their jobs will be identified and mapped to the user profiles if they are assigned multiple

roles. Positive testing will verify the users have access to the pages and functions they need. Negative testing will verify that users do not have access to data that is not required for their job.

This includes the following:

- Project Resources
- Entrance and Exit Criteria
- Types of Testing to be Utilized
- Required Test Environments
- Defect Tracking
- Scheduled Deliverables

Project Resources

The following resources have been identified as critical to the success of the testing effort:

Role	Responsibilities	Resource Name(s)
QA Lead	<ul style="list-style-type: none"> ▪ Lead testing activities ▪ Write Test Strategy ▪ Write Test Plan ▪ Write Test Cases ▪ Execute Test Cases ▪ Automate Test Scripts ▪ Find, report, and track defects ▪ Communicate Results ▪ Estimate test effort ▪ Final QA Report 	Jeff Guhin
Testers	<ul style="list-style-type: none"> ▪ Write Test Cases ▪ Execute Test Cases ▪ Automate Test scripts ▪ Execute automated scripts ▪ Find, report and track defects ▪ Measure test effort ▪ Communicate results 	Gary Gunue Todd Dodd
Project Manager/Other Management	<ul style="list-style-type: none"> ▪ Provide overall project management ▪ Accountability for all project decisions ▪ Direct activities of the project team members ▪ Interfacing with project sponsor and linkage projects. ▪ Plan tasks for the project ▪ Manages the project team ▪ Reports and communicates project status and progress ▪ Mediation of issues ▪ High-Level problem solving 	Tom Cruise Ferrah Faucet
Developers	<ul style="list-style-type: none"> ▪ Unit testing of code prior to moving to QA ▪ Deliver complete builds of the application ▪ Provide Testers with feedback regarding changes, new functionality ▪ Provide expertise and knowledge of the application-under-test ▪ Resolve assigned defects 	Grahm Fisher

Business Analysts	<ul style="list-style-type: none"> ▪ Gather project expectations from the business ▪ Compile Business Requirements ▪ Create Use Cases ▪ Liaison between IT and the Business ▪ Go-to person for clarification of business requirements 	Edward Grant
Operations Support	<ul style="list-style-type: none"> ▪ Deploy and communicate the status of new builds in QA environments ▪ Deploy and communicate the status of 3rd party software in QA environments ▪ Trouble-shooting of hardware and software elements ▪ Provide a stable testing environment ▪ In charge of launch day deployment 	Morgan Freeman
DBA	<ul style="list-style-type: none"> ▪ Provide access rights to database ▪ Assist with extraction of data for testing purposes ▪ Assist with returning database instance to a known preferred state ▪ Provide trouble-shooting and knowledge ▪ Ensure database environment is available ▪ Refresh environments 	Lenny Kravitz
Users/Business Contact	<ul style="list-style-type: none"> ▪ Describe and review Business Requirements ▪ Describe and review user profiles ▪ Perform User Acceptance Testing (UAT) ▪ Provides information needed to clarify issues ▪ Selects testers for user acceptance testing and manages user acceptance testing 	Emilio Estevez
Network Administrator	<ul style="list-style-type: none"> ▪ Provide network access privileges ▪ General troubleshooting and knowledge of network issues. 	

Entrance/Exit Criteria

The following entrance and exit criteria are required for movement in and out of test phases:

Test Phase	Entrance Criteria	Exit Criteria
Test Planning	Project Definition Test Strategy Business Requirements Functional Specifications Approved Hours on the Project Plan	Test Plan Approved
Test Design	Exit criteria above	Test Cases Written
Test Execution & Defect Tracking	Exit criteria above, plus: <ul style="list-style-type: none"> • Unit Testing Completed • Test Environments Validated 	As many of the Planned Test Cases Executed as possible for the time allocated. All Defect Fixes Tested
Pre-Launch Evaluation	Exit criteria above	All Defects Resolved: <ul style="list-style-type: none"> • Closed

		<ul style="list-style-type: none"> • Deferred • Rejected
Post-Launch	Exit criteria above	Final QA Report

Types of Testing to be Utilized

The table below describes several types of testing that have been considered for suitability in completing the work that falls under this test plan..

Test Type	Definition	Included in this Plan?
Security Test	User Profile Setup, Role & Permission List Setup, Process Security, Query Security, Portal Security, Security Migrations, LDAP Authentication	Yes

Test Case Table

The following table provides a list of test cases to be executed:

Coverage	Test Case Name
Human Resources Profiles	[1]Above Maximum Salary Analysis
	[1]Maintain Time Reporter Data
	[1]Add-Update Position Info
	[1>Delete EmplID
	[1]EEO-1 Report - Employer Information
	[1]Emergency Contact Report
	[1]Employee Compensation Changes Report
	[1]Employees on Leave of Absence Report
	[1]Generate Exception-Override Report
	[1]Generate Incumbent History report
	[1]Generate Indented Position report
	[1]Generate Vacant Position report
	[1]Home Address Report
	[1]Mailing Labels Report
	[1]Modify a Person
	[1]Personnel Actions History Report
	[1]Review Job Information
	[1]Active and Inactive Positions report
	[1]Salary History by Department Report
	[1]Salary History by Employee Report
	[1]Search by National ID
	[1]Temporary Employees Report
	[1]Pay Rate Change
	[1]Position History
[1]View Position Budget Status	
[1]Position Summary	
[1]Vacant Budgeted Positions	
[1]Years of Service Report	

Coverage	Test Case Name
	[1]HR - Access to North American Payroll
	[1]Benefits - Leave Accruals
	[1]Access to Workforce Admin - Job data
	[1]Enroll Time Reporter
	[1]Reporting Tools - Query Manager
Payroll Profiles	[1]01 Create Additional Pay
	[1]03 Create general deductions
	[1]07 Update Employee Federal Tax Data
	[1]10 Update Tax Distribution
	[1]11 Manage Employee Payroll Data -Termination-
	[1]14 Manage Direct Deposit
	[1]19 Manage Employee Garnishments
	[1]22 Update Paysheets
	[1]23 Create and Load Paysheets
	[1]25 Produce Payroll, Pre Calc audit
	[1]28 Produce Payroll, Calculate Pay
	[1]29 Produce Payroll, Confirm Pay
	[1]31 Create Online Checks
	[1]37 Create Direct Deposit File
	[1]38 Print Advice Forms
	[1]39 Produce Check
	[1]41 Reverse-Adjust Paycheck
	[1]43 Balance Adjustments
	[1]Access to Ceridian Extract
	[1]Setup HRMS
	[1]Manager Self Service
	[1]Reporting Tools - Query Manager
	[1]07 Update Employee State Tax Data
	[1]07 Update Employee Local Tax Data
	[1]Benefits - Leave Accruals
	[1]Time Reporting Codes - TRC
	[1]TRC Program
	[1]Adjust Paid Time
	[1]Build Schedule Calendar
	[1]Create a new schedule definition
	[1]Create a new Shift
	[1]Create a new Workday
	[1]Enroll Time Reporter
	[1]Manage Exceptions
	[1]Approve Time and Exceptions-Payable Time
	[1]Request Batch Approval Process
	[1]Request Time Administration
	[1]Process Individual Approval
	[1]Run Reports
	[1]Setup new Workgroup
	[1]View Payable Time
	[1]View Schedule Calendar
	[1]Access to Workforce Admin - Job data

Coverage	Test Case Name
	[1]Benefits - Leave Accruals
	[1]Reporting Tools - Query Manager
	[1]Access to Workforce Admin - Add person
	[1]Access to Workforce Admin - Job data
	[1]Attempt to access Job Data thru a bookmark
IT Profiles	[1]Verify Assigned Roles Against Matrix
Employee Profiles	[1]View Paycheck
	[1]Update contact info
	[1]Enter Time
	[1]Login timeout interval
Manager Profiles	[1]View Paycheck
	[1]Update contact info
	[1]Enter Time
	[1]Manager-Approve Time
LDAP Integration	[1]1 Login with NT password
	[1]2 Change Password in PeopleSoft
	[1]3 Change Network Password
Record Level Auditing	TBD

Required Test Environments

There will be 1 test environment in which a full cycle of Security testing will occur. Testing in the Production environment will be a subset of the tests executed in Development.

Environment	Type of Testing	Comments
Development	Positive and Negative testing	To verify users have access to the functionality to perform their job and do not have access to confidential data.
Production	High Level regression (25% of total tests)	To verify security was implemented as required.

Defect Tracking

Identified defects will be logged into TestDirector. Once the project team has corrected a defect, the defect will be retested using the same Test Script that detected the defect. Validated fixes will be entered into TestDirector. Accurate defect status data will be maintained in TestDirector.

Scheduled Deliverables

Task/Deliverable	Resources	Comments	Projected Start/End Dates
Test Plan Completed	Jeff Guhin		12/09/05
Test Cases Planned	Jeff Guhin		12/05/05
Test Cases Created	Jeff Guhin	Tracked in TestDirector	12/05/05- 12/15/05
Test Cases Executed	Jeff Guhin Todd Dodd Gary Smithey	Tracked in TestDirector	12/12/05 – 12/17/05
Defect Management	Jeff Guhin	Submitted and tracked in TestDirector	12/12/05 – 12/17/05
Test Results	Jeff Guhin	Tracked in TestDirector	12/18/05
Launch Support	Jeff Guhin		12/16/2005 – 12/23/2005
Final QA Report	Jeff Guhin		01/06/2006- 01/06/2006

Approvals

Name/Title	Signature	Date
Name/Project Manager Tom Cruise		
Name/Project Sponsor Ann Sanchez		
Name/ HR Project Lead Ferrah Faucet		
Name / Payroll Project Lead Emilio Estevez		
Name/Technical Architect Edward Grant		
Name / Business Analyst Grahm Fisher		
Name/Business Analyst Morgan Freeman		
Name/Business Analyst Lenny Kravitz		
Name/QA Lead Jeff Guhin		

Revision History

Date	Version	Description	Author
12/09/05	1.0	First draft	Jeff Guhin
12/10/05	1.1	Added appendix	Jeff Guhin

Appendix A

Date: November 12, 2005
To: Rebecca Snarski
From: Jeff Guhin
Subject: Proposal for the Oracle/PeopleSoft Human Capital Management application module security strategy for XYZ Company.

Introduction

XYZ Company currently has multiple legacy systems used in production for Human Resources and Payroll applications. These systems are not fully integrated with each other which results in duplicate records, inconsistent naming conventions, and intensive manual corrections.

An Enterprise Resource Planning (ERP), package has been purchased from Oracle/PeopleSoft. ERP is a business management system that integrates core business processes including planning, sales, marketing, order tracking, customer service, finance and human resources. The ERP system will be implemented one module at a time. The first module titled Human Capital Management (HCM), will launch December 18, 2005.

The Oracle/PeopleSoft HCM application will help HR meet organizational objectives:

- Enable HR to serve the organization more strategically
- Improve service to employees and managers
- Reduce Administrative costs
- Eliminate process steps, approvals, and paper-based forms
- Increase employee satisfaction
- Enable manager access to data for improved decision making
- Increase information access
- Implement “best practice” process out of the box

Problem

The Oracle/PeopleSoft HCM solution should have stringent security measures to prevent unauthorized end users from abusing their roles within the application. PeopleSoft defines security by providing access to data and tools users’ need to do their job.

Access and manipulation of data need to be carefully controlled and tested. An employee entering customer records should not have the permission to view employee payroll data. In the Human Resources solution of an ERP system an employee should not have the rights to approve his/her own performance appraisal.

As with any core business application, security is critical to Oracle/PeopleSoft HCM. Every department should not be allowed access to all the functions or all the data of all the applications.

Solution

The implementation date does not allow adequate time to properly design a sophisticated security model. The organizations accelerated approach demands a temporary security strategy to convert the existing production data into the new system and allow the human resources and payroll departments access to get their tasks done. These departments currently have full read/write access to all data in their applications. This access will propagate into the new system for a limited time. Once the conversion data is accurately verified roles and permission lists will be assigned to the appropriate user profiles defined by the long term security model.

Conclusion

The initial HCM implementation will grant all existing application users the same access they currently have. A sophisticated security model would be in development for implementation at a later date that would cover the following security topics:

Permission Lists

- Tailored Approach
- Mixed Modular Approach

Role Setup

- Base User Profile
- Dynamic Roles
- Row Level Security
- Process Security
- Definition Security

Authentication

- LDAP
- SSO
- PDI

Data Audit Requirements

- Field Level Auditing
- Record Level Auditing
- Database Level Auditing
- Reporting Audit Information

The decision to delay the sophisticated security model ensures the scalability of the system for future growth. The primary objective is to get the Oracle/PeopleSoft HCM module in production and allow the existing users the same access they currently have.

References

Carter, J. (2004). The Expert Guide to PeopleSoft Security. Lincoln, NE: iUniverse, Inc.

Benge, J., MacNaughton, J., Hussain F. (2004). Securing Your PeopleSoft Application Environment

Oracle. All Rights reserved. (2005). Enterprise HRMS Row Level Security in Release 8.9; An Oracle Red Paper

Oracle. All Rights reserved. (2005). Learn Oracle From Oracle. Security Guide. Redwood Shores, CA: Oracle Corporation

Oracle. All Rights reserved. (2005). Learn Oracle From Oracle. Upgrading Your PeopleSoft System. Redwood Shores, CA: Oracle Corporation