Oracle PeopleSoft Annual Manager Access Approval Process for Payroll and TAM

Version 1.8

Approved: December 2015
by Teri Augustine

Information Management Division

Revision History

The revision history identifies the version number, the date of change, a brief description on the change, and sections impacted by the change. The document is considered final upon final approval of the IMD ERP Section Director.

The revision history table (below) captures each change made to this document.

Version	Change Date	Description of change	Affected Section(s)	Prepared by
.5	11/5/2015	Feedback from P. Summerbell, D. Houston, M. Dubey. Approved pending T. Calderon notification of HR Officers role in process.	Section 5 to clarify HROs may work with BSCs, DAMs or DOMs.	A. Wade
1.0	11/24/2015	T. Augustine approved on 11/12. Approved 11/5 by HRD and FIN representatives.	All sections	A. Wade
1.5	12/10/2015	Feedback from T. Jennings. T. Augustine approved.	1, 4, 5 and 5.1	A. Wade
1.8	11/8/2016	Update schedule. Change ITD to IMD. Change Security Lead to Security Representative.	1, 4 and 5	A. Wade

Table of Contents

Revision History 2
1. Purpose 4
2. Scope 4
3. TxDOT PeopleSoft User Authorization 4
4. Process Triggers 4
5. Audit Process for Manager Approval 4
5.1 Payroll and TAM Annual Manager Access Approval Audit Process Workflow 6
5.2 Payroll and TAM Annual Manager Access Approval Audit Process Narrative 7
6. Security Contact 8

1. Purpose

This document provides guidance and procedures for the annual security approvals audits for the Payroll and Talent Acquisition Management (TAM) modules of Human Capital Management (HCM) in the Texas Department of Transportation's (TxDOT's) PeopleSoft application. The processes documented herein formalize the review process and procedures to be followed by the Information Management Division (IMD), the Human Resource Officers (HROs) and TxDOT managers.

2. Scope

The scope of the Oracle PeopleSoft Annual Approval Audit Process for Payroll and TAM is to validate current roles assigned to user profiles. The PeopleSoft application at TxDOT is configured as a role-based application, this document focuses on the concept of PeopleSoft user profile and roles.

3. TxDOT PeopleSoft User Authorization

The TxDOT PeopleSoft application employs a security matrix that uses distinct security user profiles, configured with roles designed to limit user access to required application features.

Under this configuration, access to PeopleSoft is defined through the user's profile. Based on job function and manager approval, the user profile is linked to one or more roles. A user profile inherits most of its basic permissions through roles. The number of roles that a user has depends on his/her job responsibilities.

4. Process Triggers

All TxDOT PeopleSoft users are granted base roles upon user profile provisioning. Any additional access provisioning is initiated by the submission of a Role Request through TxDOTNow, TxDOT's Information Technology helpdesk portal. TxDOTNow workflow requires manager approval before the request is sent to IMD PeopleSoft Security for fulfilment. PeopleSoft Security validates each request against access criteria provided by the business-area subject matter experts (SMEs). Any request that does not meet access constraints is not provisioned.

5. Audit Process for Manager Approval

This audit is performed annually for the agency in November.

- November – for X_PY_DDO_COORD, X_TAM_HIRING_TEAM, and X_TAM_HIRING_SUPPORT

The audit validates the assignment of the X_PY_DDO_COORD, X_TAM_HIRING_TEAM, and X_TAM_HIRING_SUPPORT roles provisioned to each TxDOT employee. A PeopleSoft Security representative runs the report to pull a list of TxDOT employees, PeopleSoft roles, and current manager by D/D/O. The reports are sent to the HRO responsible for the D/D/O. The report will also include a description of each role and the functions permitted by the role.

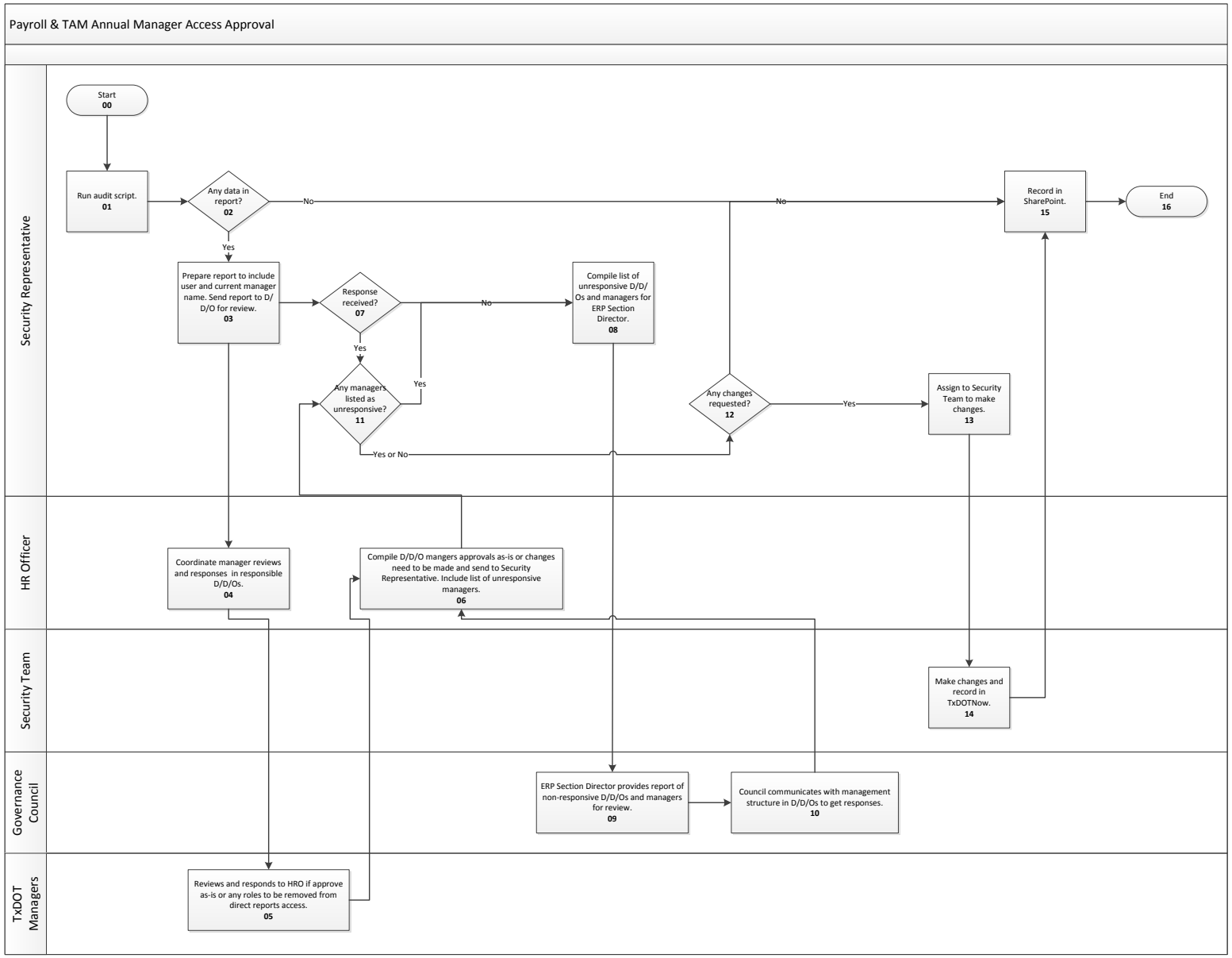
The HRO is responsible for coordinating manager reviews of user roles by directly contacting the managers or working with Business Service Coordinators (BSCs), Division Administrative Managers (DAMs) or Division Operations Managers (DOMs). The TxDOT manager is responsible for reviewing the description and functions permitted by PeopleSoft roles and the roles currently assigned to his/her direct reports. The TxDOT manager must respond to the HRO with approval as-is or any role deletions within 2 weeks. Any new role requests must follow the standard TxDOTNow ticket process.

The HRO will compile all manager responses and send to the PeopleSoft Security representative within 1 month of initial receipt. The PeopleSoft Security representative will coordinate with the PeopleSoft Security team to make any requested removals.

Reports sent and responses are tracked in SharePoint. All changes made are tracked by entering a TxDOTNow ticket.

Figure 5.1 and Table 5.2 illustrate the process for this audit.

5.1 Payroll and TAM Annual Manager Access Approval Audit Process Workflow



5.2 Payroll and TAM Annual Manager Access Approval Audit Process Narrative

Step	Responsible	Description
00	Security Representative	Start process
01	Security Representative	Run ELM/HCM Role Access Audit Report in HCMPD on first business day of October.
02	Security Representative	Review report for data for roles X_PY_DDO_COORD, X_TAM_HIRING_TEAM and X_TAM_HIRING_SUPPORT. Are there any results from the report? • If Yes, go to Step 3 • If No, go to Step 15
03	Security Representative	Prepare reports for HROs. Include user name, DDO and manager name. Also provide HRO with description of roles and functions permitted by each role for the review by managers.
04	HRO	Coordinates reviews by managers of direct reports PeopleSoft roles for D/D/O.
05	TxDOT Managers	Reviews report and responds to HRO if approve access as-is or any removals requested within 2 weeks of receiving report.
06	HRO	Follows-up with managers as needed and compiles list of responses. Sends list of responses, including non-responsive managers, to PeopleSoft Security Representative. HRO to send information within
07	Security Representative	Has the security team received a response from the HRO by first business day of month after sending report? • If Yes, go to 11 • If No, go to 08
08	Security Representative	Prepare report of non-responsive D/D/Os and managers for ERP Section Director.
09	ERP Section Director	ERP Section Director presents non-response report to HRD Division Director as part of Security update.
10	HRD DD/ERP Section Director	HRD Division Director and ERP Section Director coordinates with management to facilitate response for audits.
11	Security Representative	Are any managers listed as unresponsive? • If Yes, go to 8 • If Yes or No, go to 12
12	Security Representative	Have any managers requested access removals? • If Yes, go to 13 • If No, go to 15
13	Security Representative	Assign access changes to a member of the Security team for completion.
14	Security Team	Make requested security changes and document changes for each user in a separate TxDOTNow ticket.
15	Security Representative	Update SharePoint record with responses received and actions taken.

16	Security Representative	End Process.

6. Security Contact

For general security questions contact the PeopleSoft Support Center via TxDOTNow or at 512-CONNECT. To run off-cycle security audits contact the PeopleSoft Security Lead, Hanh Le. To obtain more data for audits contact a PeopleSoft developer.

PeopleSoft Security Lead:

Hanh Le	Hanh.Le@txdot.gov

PeopleSoft Developers

Hanh Le	Hanh.Le@txdot.gov
Brian Wetzig	Brian.Wetzig@txdot.gov
Patty Ybarra	Patty.Ybarra@txdot.gov
Ben Hayes	Ben.Hayes@txdot.gov