



Oracle PeopleSoft Security Audit Process for Payroll and TAM

Version 1.5

Approved: December 2015
by Teri Augustine

ERP Section, Information Technology 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 ITD 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
.1	10/27/15	Changes based on feedback from J. Pennington, H. Le and M. McGillivray	All sections	A. Wade
.5	11/5/15	Changes based on feedback from P. Summerbell, D. Houston, and M. Dubey. Document approved.	Section 6 and 6.1 to clarify any role change, add or delete audited	A. Wade
1.0	11/24/15	T. Augustine approved on 11/12. Approved 11/5 by HRD and FIN representatives.	All Sections	A. Wade
1.5	12/10/15	Feedback from T. Jennings. T. Augustine approved.	1, 4, 5, 5.2 and 7	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 Data Access Permission	5
5.1 Payroll and TAM Data Access Permission Audit Process Workflow	6
5.2 Payroll and TAM Data Access Permission Audit Process Narrative	7
6. Audit Process for Role Access	8
6.1 Payroll and TAM Monthly Security Audit Process Workflow	9
6.2 Payroll and TAM Monthly Security Audit Process Narrative	10
7. Security Contact	11

1. Purpose

This document provides guidance and procedures for the monthly security access reviews 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 Technology Division (ITD) Enterprise Resource Planning (ERP) Section and the subject matter experts (SMEs) identified in the business offices of primary responsibility.

2. Scope

The scope of the Oracle PeopleSoft Monthly Security Audit Process for Payroll and TAM is to validate accesses 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, roles, and data access permission.

3. TxDOT PeopleSoft User Authorization

The TxDOT PeopleSoft application employs a security matrix that uses distinct security user profiles, configured with roles and data access permissions, designed to limit user access to required application features. One can view this PeopleSoft security matrix as a three layer- structure with user profiles at the top layers, roles, and various data access permission as the last layer. Data access permissions are used minimally throughout the application as needed for TAM access for non-managers and D/D/O reporting.

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.

The data access permission determines the scope of the data, such as entire agency or a single district.

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 ITD PeopleSoft Security for fulfilment. PeopleSoft Security validates each request against access criteria provided by the business-area SMEs. Any request that does not meet access constraints is not provisioned.

To validate the provisioning of roles and data access permission reviews are performed monthly. Access reviews can also be triggered off-cycle by the SME, PeopleSoft Security team, or TxDOT top-level management.

5. Audit Process for Data Access Permission

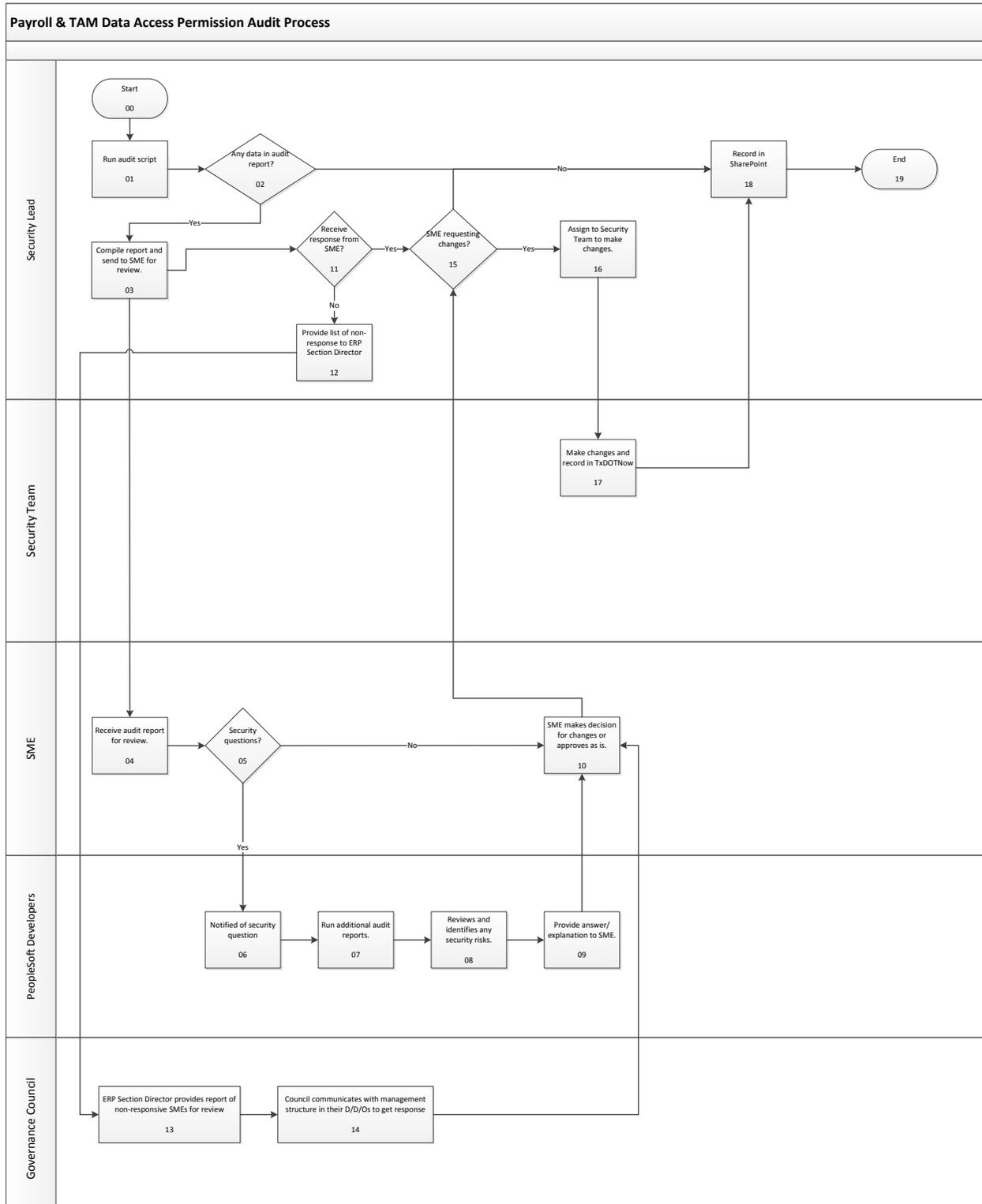
This audit is performed monthly on the first business day of the month or off-cycle as triggered. The audit validates the X_PY_DDO_COORD, X_TAM_HIRING_TEAM and X_TAM_HIRING_SUPPORT have the correct District / Division / Office (D/D/O) data access permission setup. The PeopleSoft Security team lead runs the report and sends to the SMEs to validate.

The SME is responsible for reviewing the report to identify any issues. SME must respond within 5 business days noting their approval or actions to be taken. The PeopleSoft Security team is responsible for making any changes identified by the SME. Note, non-responses will be reported to the ERP Governance Council.

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

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

5.1 Payroll and TAM Data Access Permission Audit Process Workflow



5.2 Payroll and TAM Data Access Permission Audit Process Narrative

Step	Responsible	Description
00	Security Lead	Start process
01	Security Lead	Run ELM/HCM Role Access Audit Report in HCMPD on the first business day of the month to show users with access.
02	Security Lead	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? <ul style="list-style-type: none"> • If Yes, go to Step 3 • If No, go to Step 18
03	Security Lead	Compile report and sent to SME for review. (See section 7 for list of SMEs).
04	SME	Receives audit report on 1 st business day of the month. SME reviews the reports by validating accesses.
05	SME	Is additional security verification information needed to validate user's access? <ul style="list-style-type: none"> • If Yes, go to 6 • If No, go to 10
06	PeopleSoft Developer	Receive notice of SME security question via email or phone call.
07	PeopleSoft Developer	Verify by running necessary scripts/query/report. May include running more audit trails based on question or issue presented by the SME and if potential security risk is identified.
08	PeopleSoft Developer	Analyzes results, including collaborating with Security Lead and Accenture.
09	PeopleSoft Developer	Provide results and analysis to SME in 2 business days.
10	SME	Respond to Security Lead if report is approved as is or any access changes that need to be made.
11	Security Lead	Has the security team received a response from the SME in 5 business days? <ul style="list-style-type: none"> • If Yes, go to 15 • If No, go to 12
12	Security Lead	Prepare report of non-responsive SMEs and security access that has not been reviewed.
13	Governance Council	ERP Section Director presents non-response report to Council for review as part of Security update.
14	Governance Council	Council members coordinate in their respective D/D/Os to facilitate SME response for audits.
15	Security Lead	Has the SME requested access changes? <ul style="list-style-type: none"> • If Yes, go to 16 • If No, go to 18
16	Security Lead	Assign access changes to a member of the Security team for completion.
17	Security Team	Make requested security changes and document changes for each user in a separate TxDOTNow ticket.
18	Security Lead	Update SharePoint record with responses received and actions taken.
19	Security Lead	End Process.

6. Audit Process for Role Access

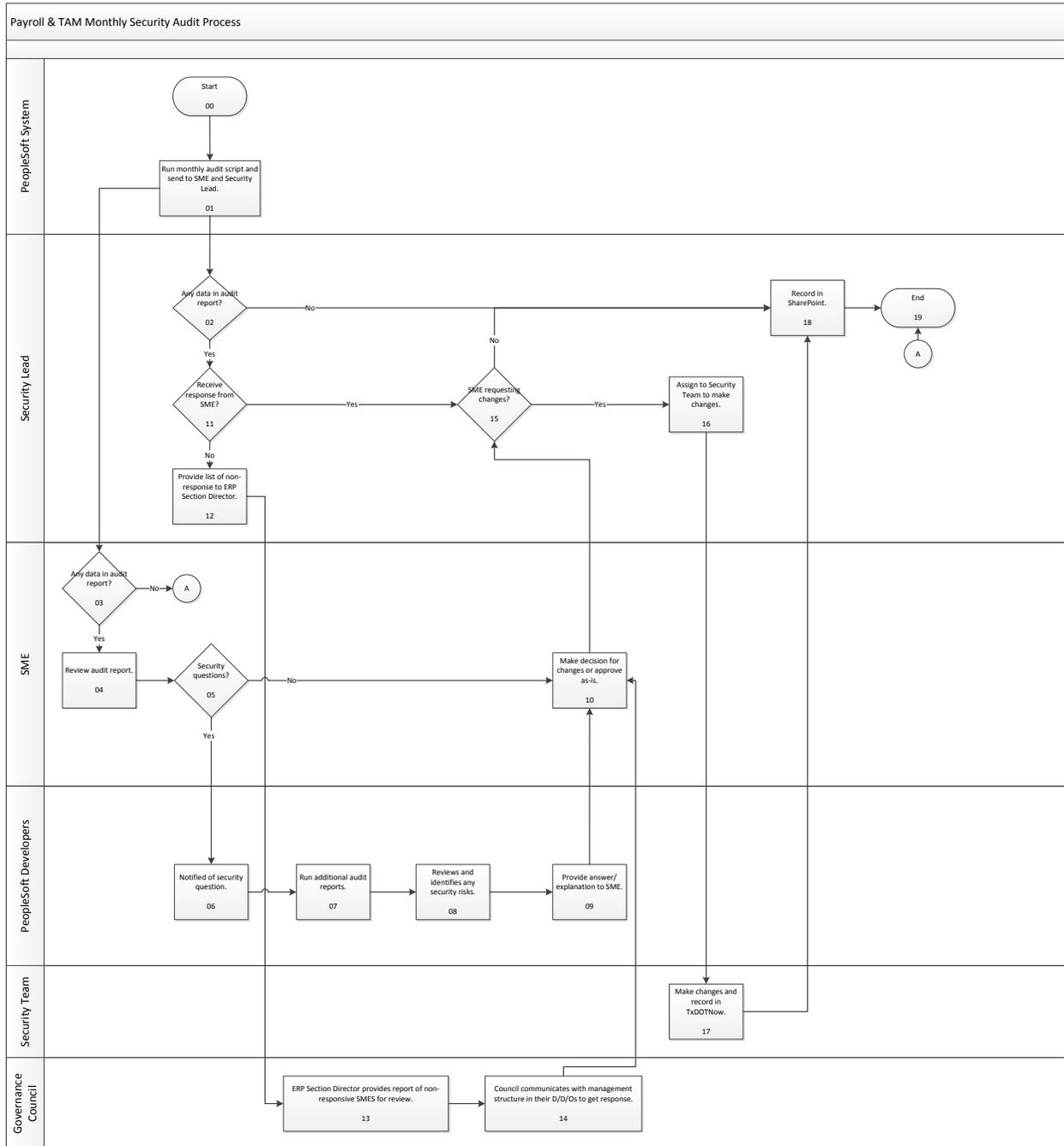
This audit is performed monthly. The monthly role access audit process is scheduled to run on the first day of each month. The audit report is sent to the SME automatically by the system. The report lists all the Payroll and TAM roles added, removed or updated in the past month including the user name, access, all roles assigned to user, who provisioned the access, action date/time, and user's job title.

The SME is responsible for reviewing the report to identify any issues with segregation of duties or excessive access. SME must report back to PeopleSoft Security team lead within 5 business days noting their approval of all users granted access to Payroll/TAM or listing actions to be performed. The PeopleSoft Security team is responsible for making any changes identified by the SME. Note, non-responses will be reported to the ERP Governance Council.

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

Figure 6.1 and Table 6.1 illustrate the process for this audit.

6.1 Payroll and TAM Monthly Security Audit Process Workflow



6.2 Payroll and TAM Monthly Security Audit Process Narrative

Step	Responsible	Description
00	PeopleSoft system	Start process
01	PeopleSoft system	Run automated monthly audit report for all Payroll and TAM roles added in the previous month on the 1 st business day of the month.
02	Security Lead	Review report for any user access changes to Payroll or TAM roles in the previous month. Are there user access changes? <ul style="list-style-type: none"> • If Yes, go to Step 11 • If No, go to Step 18
03	SME	Receives audit report on 1 st business day of the month. Review report for any user access changes to Payroll or TAM roles in the previous month. Are there user access changes? <ul style="list-style-type: none"> • If Yes, go to Step 4 • If No, go to Step 19
04	SME	SME reviews the report by validating accesses being added, updated, or changed and comparing to job duties. SME evaluates the user's role access & identifies any segregation of duties or excessive access.
05	SME	Is additional security verification information needed to validate user's access? <ul style="list-style-type: none"> • If Yes, go to 6 • If No, go to 10
06	PeopleSoft Developer	Receive notice of SME security question via email or phone call.
07	PeopleSoft Developer	Verify by running necessary scripts/query/report. May include running more audit trails based on question or issue presented by the SME and if potential security risk is identified.
08	PeopleSoft Developer	Analyzes results, including collaborating with Security Lead and Accenture.
09	PeopleSoft Developer	Provide results and analysis to SME in 2 business days.
10	SME	Respond to Security Lead if report is approved as-is or any access changes that need to be made.
11	Security Lead	Has the security team received a response from the SME in 5 business days? <ul style="list-style-type: none"> • If Yes, go to 15 • If No, go to 12
12	Security Lead	Prepare report of non-responsive SMEs and security access that has not been reviewed.
13	Governance Council	ERP Section Director presents non-response report to Council for review as part of Security update.
14	Governance Council	Council members coordinate in their respective D/D/Os to facilitate SME response for audits.
15	Security Lead	Has the SME requested access changes? <ul style="list-style-type: none"> • If Yes, go to 16 • If No, go to 18
16	Security Lead	Assign access changes to a member of the Security team for completion.
17	Security Team	Make requested security changes and document changes for each user in a separate TxDOTNow ticket.
18	Security Lead	Update SharePoint record with responses received and actions taken.
19	Security Lead	End Process.

7. 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

Jennifer Pennington Jennifer.Pennington@txdot.gov

Brian Wetzig Brian.Wetzig@txdot.gov

Patty Ybarra Patty.Ybarra@txdot.gov

Ben Hayes Ben.Hayes@txdot.gov

SMEs:

Paul Summerbell Paul.Summerbell@txdot.gov

David Houston David.J.Houston@txdot.gov

Mary Dubey Mary.Dubey@txdot.gov

Sue Park Sue.Park@txdot.gov

Connie Hoffman Connie.Hofmann@txdot.gov

Leslie Sanders Leslie.Sanders@txdot.gov