Objective

Summary Results
Testing consisted of an evaluation of 7 MAPs to determine if corrective actions were implemented as agreed.

<table>
<thead>
<tr>
<th>MAP Status</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 Open</td>
<td>Corrective actions that require completion to address identified risks from the original audit report.</td>
</tr>
<tr>
<td>4 Closed</td>
<td>Corrective actions have been completed.</td>
</tr>
</tbody>
</table>

Scope
The scope of this engagement included Information Management Division's (IMD) current software and operating procedures used for securing TxDOT resources in password re-sets, hardware sanitization, software installations, and access removal. For access removal testing, employees that were terminated between August to September 2015 and March 2016 were selected. Testing was conducted in Beaumont, Dallas, and Houston districts to determine if hardware was sanitized properly.

The engagement was performed by Keith Laird and Jill Emery (Engagement Lead). The engagement was conducted during the period from February 22, 2016 to May 10, 2016.

Methodology
The methodology used to complete the objective of this engagement included:
- Reviewed Information Management Division's (IMD) Software Management Project Plan to verify it includes a comprehensive software inventory and license library plan
- Identified if a total license count was determined
- Tested the installation of software on a select desktop to assess if administrative rights were properly removed
- Obtained PeopleSoft list of terminated employees to determine automatic notification to IMD of terminated employees
- Assessed the off-boarding process to determine if System Administrators are provided immediate notification of termination
- Tested telephone password resets through auditor observation of 3 TxDOT contractors to determine if contractors were appropriately identified prior to password reset
- Obtained and reviewed IMD’s Major Equipment System Salvage and Hard Drive Sanitation Process and verified it contained instructions for transfer and sanitization of surplus hard drives, along with requiring a label with two signatures (one who sanitized, the other who tested success of sanitization)
- Observed surplus hard drives in 3 districts to determine labels were used and signed by two independent persons
Background
This report is prepared for the Texas Transportation Commission and for the Administration and Management of TxDOT. The report presents the results of the General Controls Review - IT Follow-Up engagement which was conducted as part of the Fiscal Year 2016 Audit Plan.

The Information Management Division’s (IMD) goal is to support TxDOT’s mission by establishing a reliable, secure, and simplified IT environment that progressively moves towards industry standards and meets evolving needs of the agency. To support that mission, IMD has gone through significant changes, including the outsourcing of IT support to a third-party service provider, the privatization of certain IT services, and refreshing computers, servers, and other equipment. IMD has also enhanced their internal procedures to verify the identity of a user prior to resetting passwords, as well as, monitoring user access during termination to ensure access is removed.

We conducted this follow-up engagement in accordance with Generally Accepted Government Auditing Standards and in conformance with the International Standards for the Professional Practice of Internal Auditing. Those standards require that we plan and perform the engagement to obtain sufficient, appropriate evidence to provide a reasonable basis for our conclusions based on our engagement objective. Recommendations to mitigate risks identified were previously provided to management during the original engagement to assist in the formulation of the management action plans referenced in this report. The Internal Audit Division uses the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control – Integrated Framework version 2013.
Detailed MAP Follow-Up Status

MAP Status: Open
Corrective actions that require completion to address identified risks from the original audit report.

**Original Audit Finding Number 1:** Process to Ensure Software is Properly Licensed and Approved

**MAP Owner:** Margaret Dixon, Risk and Security Strategy Manager, Information Management Division (IMD)

**MAP 1.2:** Working with divisions, districts and regions, IMD will construct a Software Management project plan to estimate the resource and timeline to implement a comprehensive software inventory and license library.*

IMD will collect an installation baseline to perform a risk based software license count, assisted by the purchase of an additional software tool. Ultimately, it will then be necessary to secure automated license monitoring software or to investigate alternatives for augmenting the current System Center Configuration Manager (SCCM) capabilities.

*Items that are italicized were considered complete.

**Original Completion Date:** April 15, 2013
**Revised Completion Date:** March 15, 2017

**FMAP 1.1:** IMD is using Avecto to prevent users from installing unauthorized software. The 462 computers identified as not having Avecto installed will be reviewed, and a plan will be developed to determine whether Avecto is needed on those computers.

**Original Completion Date:** January 15, 2015
**Revised Completion Date:** September 15, 2016

**Original Audit Finding Number 5:** Un-sanitized Hard Drives in Surplus Equipment

**MAP Owner:** Margaret Dixon, Risk and Security Strategy Manager, Information Management Division (IMD)

**FMAP 5.1:** IMD has instituted a revised MES Salvage & Hard Drive Sanitation Process that requires MES transfer and hard drive wipe/sanitation process instructions. Those instructions include an updated salvage label that requires the signature of the person performing the disk sanitization and of the person testing to confirm that all data is removed and a timeframe on when the hard drives need to be sanitized. The instructions will be part of our Service Manager manual. IMD will also implement a project that will pick up spare inventory from the warehouses for disposal, which will include a secure wipe if needed. IMD will revise the MES Salvage & Hard Drive Sanitation Process to provide direction for sites that do not have the ability to obtain two signatures.

**Original Completion Date:** October 15, 2014
**Revised Completion Date:** February 15, 2017
MAP Status: Closed
Corrective actions have been completed.

<table>
<thead>
<tr>
<th>Original Audit Finding Number 2: Documented and Approved Information Resources Security Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAP Owner: Margaret Dixon, Risk and Security Strategy Manager, Information Management Division (IMD)</td>
</tr>
</tbody>
</table>

MAP 2.1*: IMD currently has the IT Security Manual and IT Security Guide that captures many of the TAC requirements. Previously these two manuals were viewed as being adequate to meet the TAC requirements and previous IT audits specifically in this area. IMD will create a master security program document that will serve as the summary of each of the current security program initiatives. The Chief Information Officer will review this single document to ensure it complies prior to it being sent to the Executive Director for review and signature annually. IMD is currently developing an agency wide business continuity program which will include business impact analysis for each key area of the business. These business impact analyses will identify both mission critical applications and mission critical core IT functions. The plan will include the following components and will be implemented by the dates indicated. A draft program will be established in April 2013 and individual components of that program will be delivered as completed based on the schedule below:

- Authorize Changes to Data
- Publish Draft Information Security Program Plan
- Assurance of Data Integrity
- Definition of Mission Critical Applications
- Review of the Agency’s Compliance with the TAC Security Standards
- Completion of an IT Risk Assessment from a Business and Security Aspect
- Completion of a Business Impact Analysis
- Completion of a Business Continuity Plan
- Assurance of Adequate Controls and Separation of Duties
- Report Annually to the Agency Head or their Designee the status and Effectiveness of security controls
- Review and Approval by the State Agency Head Or His/Her Designated Representative – December 2013

*MAP is being closed in this report due to the risk mitigation/remediation plan being transferred to TAC 202 Reporting audit – Completion Date: December 15, 2017
Original Audit Finding Number 3: Terminated Employee Access to Mainframe System  
**MAP Owner:** Margaret Dixon, Risk and Security Strategy Manager, Information Management Division (IMD)

**MAP 3.1:** IMD will enhance the current compliance monitoring system to include daily monitoring of terminated employees. Monitoring will include mainframe, LAN, and key applications which do not utilize existing LAN accounts for authentication (i.e., SiteManager). IMD will also work with the Human Resources Division to develop an improved off-boarding process to provide immediate notification to the Security Administrators when an employee terminates.

<table>
<thead>
<tr>
<th>Original Completion Date</th>
<th>August 15, 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revised Completion Date</td>
<td>October 15, 2014</td>
</tr>
<tr>
<td>Actual Completion Date</td>
<td>March 15, 2016</td>
</tr>
</tbody>
</table>

Original Audit Finding Number 4: Verification of Novell and/or Windows Password Resets  
**MAP Owner:** Margaret Dixon, Transformation Management Lead – IT Security Risk and Security Strategy Manager, Information Management Division (IMD)

**MAP 4.2:** IMD is establishing a process whereby only support staff with be granted extremely limited HR Online access such that they would be able to view the last four digits of a TxDOT employees’ Social Security Number and query the caller for those four digits to confirm their identity before resetting a password. We will use this to verify the identity of an employee over the phone before resetting their password. In addition, we are investigating a means for verifying contractors since they are not in the HR Online system.

<table>
<thead>
<tr>
<th>Original Completion Date</th>
<th>May 15, 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revised Completion Date</td>
<td>July 27, 2015</td>
</tr>
</tbody>
</table>

Original Audit Finding Number 5: Un-sanitized Hard Drives in Surplus Equipment  
**MAP Owner:** Andrew Chavez, Director, Support Services Division

**FMAP 5.2:** The Support Services Division (SSD) will update current guidelines to the staff handling computer hardware for surplus to verify that the label on the equipment indicates two signatures.

<table>
<thead>
<tr>
<th>Original Completion Date</th>
<th>October 15, 2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actual Completion Date</td>
<td>November 7, 2016</td>
</tr>
</tbody>
</table>

**Closing Comments**
The results of this MAP Follow-Up engagement were discussed with Information Management Division on August 3, 2016, and Support Services Divisions on August 5, 2016. The Internal Audit team appreciates the cooperation and assistance received from the Information Management and Support Services Divisions during this engagement.