Texas Department of Licensing and Regulation

IA #03-2025 Internal Audit Report over IT Services

Follow Up Procedures

September 23, 2025

weaver

Assurance • Tax • Advisory

CONFIDENTIAL - GOVERNMENT CODE §552.139 - This report contains confidential information and is protected from disclosure under §552.139 of the Texas Government Code and may only be released to law enforcement, the state auditor's office, and agency or elected officials designated by the agency. It may not be shared, released or otherwise disclosed.

CONTENTS

Page

Audit Report Transmittal Letter to the Commission....1

Background....2

Follow-Up Procedures Scope and Objective....2

Executive Summary....3

Conclusion....3

Detailed Follow-Up Results, Findings, Recommendations and Management Response....4

Appendix....11

weaver
Assurance • Tax • Advisory

Commissioners of the
Texas Department of Licensing and Regulation
920 Colorado Street
Austin, TX 78701

This report presents the results of the internal audit follow-up procedures performed for the Texas Department of Licensing and Regulation (TDLR) during June 2025, through September 2025 related to the findings identified in the Internal Audit Report over Information Technology Services issued July 22, 2024.

The objective of these follow-up procedures was to validate that adequate corrective action has been taken to remediate the issues identified in the 2024 Internal Audit Report over Information Technology Services.

To accomplish this objective, we conducted interviews with key personnel responsible for processes over Information Technology Services. We also reviewed documentation and performed specific testing procedures to validate actions taken. Procedures were performed remotely and completed in September 2025.

The following report summarizes the findings identified, risks to the organization, and recommendations for improvement and management's responses.

Weaver and Tidwell, L.L.P.

WEAVER AND TIDWELL, L.L.P.

Austin, Texas
September 23, 2025

CONFIDENTIAL - GOVERNMENT CODE §552.139 - This report contains confidential information and is protected from disclosure under §552.139 of the Texas Government Code and may only be released to law enforcement, the state auditor's office, and agency or elected officials designated by the agency. It may not be shared, released or otherwise disclosed.

Texas Department of Licensing and Regulation

Audit Follow-Up Procedures Report Over Information Technology Services
September 23, 2025

Background

In fiscal year 2024, an internal audit over Information Technology Services was completed. The internal audit report identified thirteen findings within the processes supporting Information Technology Services. The count of total findings per risk level were:

- Seven high risk findings
- Four moderate risk findings
- Two low risk findings

The fiscal year 2025 Audit Plan included performing procedures to validate that TDLR management has taken steps to address the prior year's audit findings.

Follow-Up Procedures Scope and Objective

The follow-up procedures focused on the remediation efforts taken by TDLR management to address the findings in the 2024 internal audit over Information Technology Services, and to validate that appropriate corrective action had been taken.

Our procedures included inquiring with key personnel responsible for Information Technology Services, examining existing documentation, and evaluating if corrective action had been taken. Our coverage period was from the implementation date of the remediation through September 2025. We evaluated the corrective action taken by management to address the findings identified in the audit report.

Texas Department of Licensing and Regulation

Audit Follow-Up Procedures Report Over Information Technology Services
September 23, 2025

Executive Summary

The findings from the 2024 internal audit over Information Technology Services include those items that were identified and considered to be non-compliance issues with TDLR's policies and procedures, rules and regulations required by law, or where there is a lack of procedures or internal controls in place to cover risks to TDLR. This issue could have significant financial or operational implications.

Through our interviews, review of documentation, observations, and testing, we determined that nine of the 13 findings were remediated, and that one finding was partially remediated.

Risk Rating	Total Findings	Remediated	Partially Remediated	Not Remediated
High	**7**	**5**	**1**	**1**
Moderate	**4**	**3**	**-**	**1**
Low	**2**	**1**	**-**	**1**
Total	**13**	**9**	**1**	**3**

A summary of our results, by audit objective, is provided in the table below. *See the Appendix for an overview of the Assessment and Risk Ratings.*

SCOPE AREA	RESULT
Objective: Validate that adequate corrective action has been taken to remediate the issues identified in the 2024 internal audit over Information Technology Services.	We identified that the procedures implemented by management addressed and remediated nine of 13 findings. One finding was partially remediated, and three findings were still open.

Conclusion

Based on our evaluation, TDLR has remediated nine of the 13 findings from the 2024 internal audit over Information Technology Services. For the one remaining partially remediated finding and the three findings that are not remediated, we recommend that management continue their efforts to remediate the findings.

Additional follow-up procedures will be performed in fiscal year 2026 to validate the remaining remediation efforts.

Detailed Follow-Up Results, Findings, Recommendations and Management Response

Detailed Follow-Up Results, Recommendations, and Management Response

Our procedures included interviewing key personnel within TDLR to gain an understanding of the corrective actions taken to address the findings identified in the 2024 internal audit over Information Technology Services, as well as examining supporting documentation and performing testing to validate those corrective actions. We evaluated each process in their current state.

Objective: Validate Remediation

Validate that adequate corrective action has been taken to remediate the issue identified in the 2024 internal audit over Information Technology Services.

Finding 1 – Moderate – Change Management: TDLR does not have a policy in place to establish or document criteria defining emergency changes.

Procedure: We reviewed the TDLR Emergency Change Request Policy and determined that criteria to classify a change as Emergency were documented. Therefore, we concluded the finding was remediated.

Result: Remediated

Finding 2 – High – Change Management: Access to implement changes to the application production environments and production servers was not segregated from access to develop changes. Individuals with development access had the ability to promote their own changes to production. The impacted systems were:

- IHB
- Legal Files
- Tabs
- Tools
- TULIP
- Versa

Procedure:
We reviewed listing of users with access to develop changes and listing of users with access to implement changes to one production layer for the systems in scope. We determined that users did not have sufficient access to develop and install their own changes to production for the systems below:

- IHB (database server permissions)
- Legal Files (database server permissions)
- Tabs (application, application server permissions)
- Tools (application, application server permissions)
- TULIP (application, application server permissions)
- Versa (application permissions)

Result: Remediated

Finding 3 – Low – Software Licensing & Usage: Management has not established or documented policies governing the decommissioning of licensed software.

Procedure: We reviewed the Decommissioning Licensed Software Policy and identified that management has processes in place to be followed when a user no longer needs access to licensed software. We inspected a sample of one terminated user and noted that the user's PC was reimaged, removing access to all licensed software, as required by the Policy. Therefore, we concluded that the finding was remediated.

Result: Remediated

Finding 4 – Moderate – User Administration: System access for application accounts with access to privileged functions were not reviewed on a semi-annual or quarterly basis. Per TAC 202, "more rigorous controls commensurate to the value and potential for abuse of a type of account" should be implemented for privileged accounts.

Procedure: We determined that an account access review was performed for the systems in scope, including privileged accounts, and verified that a review of accounts with privileged access was performed for all in-scope systems:

- Active Directory
- IHB
- Legal Files
- Tabs
- Tools
- TULIP
- Versa

We determined that for two of seven systems in-scope for the finding, IHB and Legal Files, the initial review of accounts with access, including privileged functions, was completed in September 2024 (IHB) and October 2024 (Legal Files). In management’s response, it was noted that not all systems would be able to go through semi-annual privileged access reviews. As management continues with their planned system implementations that will consolidate the technology landscape, management should consider where privileged (ie, admin) permissions are reviewed on a more frequent basis.

Result: Remediated

Finding 5 – High – User Administration: Management did not perform documented reviews of user access at the database or server layer. The impacted systems were:

- IHB
- Legal Files
- Tabs
- Tools
- TULIP
- Versa

Procedure: We inspected evidence of user access review at the database layer for the systems in scope and determined that a review was performed for five of six systems; and no server level access reviews were performed. For one system, Legal Files, no evidence of review at the database layer was provided, therefore the finding was partially remediated. No review was performed over the server layer for any of the critical systems. Management should ensure that reviews are performed over all critical application production databases and servers.

Result: Partially Remediated

Management's Response: We agree. Staffing and project priorities have made this objective difficult to complete. We will obtain appropriate staffing levels and perform all access reviews as required.

Responsible Party: Chief Information Security Officer
Implementation Date: March 1, 2026

Finding 6 – Low – User Administration: Access to the on-premises data center at TDLR's Austin campus was not reviewed on a periodic basis to validate access was restricted to only those personnel who required the access to perform their assigned duties.

Procedure: We determined per inquiry with Management on July 12, 2025, that access to the on-premise data center at TDLR's Austin campus was not reviewed.

Result: Not Remediated

Management's Response: We agree. We have requested information on obtaining an access report that is delivered regularly from the Texas Facilities Commission. Should that not occur, we will perform the data center access review quarterly as required.

Responsible Party: Chief Information Security Officer
Implementation Date: December 1, 2025

Finding 7 – High – Change Management: For change requests where modifications were made after obtaining Change Advisory Board (CAB) approval, evidence of Quality Assurance (QA) testing and of further CAB approval after modification were not consistently documented and retained.

Procedure: We inspected Standard Operating Procedures documenting processes to document solution requirements, design a solution, develop a solution, test a solution, and deploy a solution, and determined that testing and approval was required for every modification performed after Change Approval Board. We determined per inquiry with Management that no modification was made to a change approved by the Change Approval Board since the implementation of the Standard Operating Procedures. As procedures were updated to require Change Advisory Board (CAB) and evidence of Quality Assurance testing after modifications to a change previously approved by the CAB, we concluded the finding was remediated.

Result: Remediated

Finding 8 – High – Project Management: Management did not perform procedures to validate the accuracy of data migrated from a legacy system to the new Versa Driver Education and Safety/Motorcycle and ATV Operation Safety system, and Management did not retain sufficient evidence to demonstrate completeness validation of migrated data.

Procedure: We obtained and reviewed TDLR's developed Standard Operating Procedure (SOP) documentation establishing validation of data migration accuracy testing to be performed. We inquired with Management and determined that no project requiring data migration was performed between the prior Internal Audit and the fieldwork period of this Internal Audit.

Result: Remediated

Finding 9 – High – User Administration: For four in-scope applications, Legal Files, Tools, TULIP, and Versa, password configuration did not meet the requirements of the Information Security Manual.

Procedure:

1. We inspected configuration settings of the Legal Files application and observed that password configuration was set to leverage network password parameters, which followed the Information Security Manual.
2. We inquired with Management and noted that Management accepted the risk of password configurations not in compliance with the Information Security Manual for the Tools and TULIP applications, as the applications are in process of being replaced in an ongoing Licensing System Replacement project.
3. We inspected password configuration settings of the Versa application and determined that system design limitations did not allow the system to retain a 15-password history as requested by the Information Security Manual, We further identified that the system was configured to retain the maximum number of passwords allowed; nine passwords.

Result: Remediated

Finding 10 – Moderate – User Administration: System access for four separated employees was not revoked in a timely manner after termination:

Procedure: We inquired with Management and determined that a peer review process was implemented to ensure that access revocation tickets were reviewed by a user other than the user responsible for performing access revocation to ensure timely and complete access revocation procedures for terminated employees.

We inspected a tracker for terminations having occurred between December 2024 and April 2025 and verified that a peer review was performed for each termination. We inspected a completed IT Services Employee Offboarding Template for one employee terminated March 7, 2025, and verified the template included a checklist for all systems in the environment, and that each item on the checklist was checked, indicating that each system was reviewed to determine whether the terminated user had access that required termination.

Result: Remediated

Finding 11 – Moderate – User Administration: A secondary review process to prevent users performing a user access review of Active Directory accounts from reviewing their own access was not in place.

Procedure: We inspected the Active Directory account reviews of divisions and determined:

- For 11 of 16 divisions, we received an email confirmation from the reviewer reviewing the Active Directory accounts of the division's users.
  - For eight of 11 email confirmations, we determined the reviewer reviewed their own access and no secondary review was performed.
  - For two of 11 email confirmations, the reviewer did not have an Active Directory account in the division, therefore an opportunity to implement a secondary review process did not exist.
  - For one of 11 email confirmations, two reviewers performed the review, however the access for one of the two reviewers showed no evidence of review.
- For the five divisions where no email confirmation was provided, we were able to conclude that a review was performed, but we were unable to identify the reviewer, therefore we were unable to determine whether the reviewer reviewed their own access. The divisions with no email provided were Contracting and Procurement, Customer Service, Education and Examination, General Counsel, and Information Security.

In evaluating whether a secondary review was performed to prevent a user's self-review, no secondary review was performed.

Result: Not Remediated

Management's Response: We agree. We will create a review log that notes the reviewer, reviewee, date and time. Additionally, the Information Security Office can work with the divisions to get the appropriate access for managers documented. This document can be referenced to assess the appropriate level of access, and any deviation will be documented in a helpdesk ticket. Managers may still review their access, and having a reference document of what access they should have will help verify correctness.

Responsible Party: Chief Information Security Officer
Implementation Date: December 1, 2025

Finding 12 – High – User Administration: Changes requested as a result of user access reviews were not consistently documented in tickets and completed timely.

Procedure: We inspected a log of tickets created between June 15, 2025, and August 1, 2025 to track changes requested as part of the user access reviews, and determined that a peer review process was implemented to ensure that access revocation tickets were reviewed by a user other than the user responsible for performing access revocation to ensure timely and complete access revocation procedures for terminated employees.

We inspected a tracker for terminations having occurred between December 2024 and April 2025 and determined that corrective actions were documented and marked as resolved.

Result: Remediated

Finding 13 – High – User Administration: Twenty-four accounts in the Tools application had inappropriate privileged access to the application. The accounts were assigned the Supervisor administrative role, which was not required to perform their responsibilities.

Procedure: We obtained a listing of 38 accounts with Supervisor administrative role in the Tools application and inquired with Management as to the appropriateness of access. Management reported the Supervisor administrative role was inappropriate for 13 of 38 accounts, therefore the finding is not remediated.

Result: Not Remediated

Management's Response: We agree. A new user role in Tools was created last year that is more appropriate for the needs of legal assistants than the Supervisor role, and 13 of the legal assistants were inadvertently not transferred to the new access role when it went into use. A helpdesk ticket was filed and all inappropriate roles have been corrected.

Responsible Party: Manager of the Licensing System Services Section
Implementation Date: September 24, 2025

Appendix

Risk Ratings

Residual risk is the risk derived from the environment after considering the mitigating effect of internal controls. The area under audit has been assessed from a residual risk level utilizing the following risk management classification system.

High

High risk findings have qualitative factors that include, but are not limited to:

- Events that threaten the Department’s achievement of strategic objectives or continued existence
- Impact of the finding could be felt outside of the Department or beyond a single function or department
- Potential material impact to operations or the Department’s finances
- Remediation requires significant involvement from senior Department management

Moderate

Moderate risk findings have qualitative factors that include, but are not limited to:

- Events that could threaten financial or operational objectives of TDLR
- Impact could be felt outside of TDLR or across more than one function of the agency
- Noticeable and possibly material impact to the operations or finances of TDLR
- Remediation efforts that will require the direct involvement of functional leader(s)
- May require senior agency management to be updated

Low

Low risk findings have qualitative factors that include, but are not limited to:

- Events that do not directly threaten TDLR’s strategic priorities
- Impact is limited to a single function within the agency
- Minimal financial or operational impact to the organization
- Require functional leader(s) to be kept updated or have other controls that help to mitigate the related risks