Texas Real Estate Commission

Report on Prior Audit Findings Follow-Up

Report # 25-003

June 18, 2025

McConnell Jones

Diverse Thinking | Unique Perspectives

Table of Contents

Audit Objectives and Focus

Executive Summary

Prior Audit Findings and Implementation Status

Key Recommendations

AUDIT OBJECTIVES AND FOCUS AREAS

Internal audit conducted a follow-up review on prior audit findings issued to determine management's implementation progress towards remediating the respective issue or internal control weakness. This follow-up audit was included in the Annual Internal Audit Plan.

We conducted this audit in conformance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained during the audit satisfied GAGAS standards.

We have not omitted pertinent information from this report.

FINDINGS STATUS SUMMARY

Finding Status	Number	Percentage of Total Findings Assessed
Fully Addressed	11	92%
Partially Addressed / Ongoing	0	8%
In-Progress	1	8%
Not Started	0	0%
Total	12	100%

Total Recommendations Remaining to be Closed: 1

DETAILED FINDINGS, RECOMMENDATIONS, AND IMPLEMENTATION STATUS

#	Audit Date	Audit # & Name	Risk Ranking	Finding	Recommendation	Status
1	February 2022	22-001 IT Asset Management	Not Rated	The 2022 asset audit should be conducted in person (employees come to the office).	Require staff to bring their Agency assets used to work remotely to the office so that asset management personnel can perform a true physical inventory of equipment. This will also provide the opportunity to tag assets and assess the condition of equipment. Personnel that cannot come to the office will need to arrange to have their items inventoried in another manner.	Fully Addressed
2	February 2022	22-001 IT Asset Management	Not Rated	Snipe-IT needs to be updated with complete information as required in the Asset Management Guides, Instructions & Procedures (SOP). We found the following: • 72 deployed assets are not assigned to a person (they assigned to a location instead); • 134 assets are deployable but are not located in the IT Storeroom; • 21 leased assets do not have a start or end lease date entered; • 447 assets do not have purchase type indicated; •700 assets do not have an inventory date indicated; and • 671 assets do not have an audit date indicated.	1. Complete the 2022 Inventory and update Snipe-IT with current information. Ensure the following are updated: a. Inventory date for all assets. The inventory field could be updated quarterly when the asset manager conducts their review. For new items this should match the date they were entered into the system and the Inventory Type should be indicated in a way to indicate this. b. Audit date for all assets. The audit field should be updated annually when the annual inventory is completed. This date should be when then full and complete inventory is completed.	Fully Addressed

DETAILED FINDINGS, RECOMMENDATIONS, AND IMPLEMENTATION STATUS

#	Audit Date	Audit # & Name	Risk Ranking	Finding	Recommendation	Status
2 Cont.	February 2022	22-001 IT Asset Management	Not Rated	Snipe-IT needs to be updated with complete information as required in the Asset Management Guides, Instructions & Procedures (SOP). We found the following: • 72 deployed assets are not assigned to a person (they assigned to a location instead); • 134 assets are deployable but are not located in the IT Storeroom; • 21 leased assets do not have a start or end lease date entered; • 447 assets do not have purchase type indicated; •700 assets do not have an inventory date indicated; and • 671 assets do not have an audit date indicated.	2. Update Snipe-it with the following information: a. Change all deployable assets to indicate they are in IT Storage. b. Enter the lease start and end date for all leased assets. c. Enter the purchase type for all assets. 3. For the assets assigned to a location, asset management should work with ITD to determine who the asset owner is and then assign the assets to them. This is because a room cannot be responsible for equipment; there should always be a person responsible for all equipment. TREC should use the “Department” field of Snipe-IT to indicate the department that is responsible for the assets in these locations. For example, if the IT Department is the asset owner for all IT equipment, then the department head must be informed that they are responsible for all the equipment.	Fully Addressed

DETAILED FINDINGS, RECOMMENDATIONS, AND IMPLEMENTATION STATUS

#	Audit Date	Audit # & Name	Risk Ranking	Finding	Recommendation	Status
3	February 2022	22-001 IT Asset Management	Not Rated	It was noted that deliveries to the agency are not always left with the mail room. There have been instance of packages/mail left in hallways, the elevators and in front of doors.	Work with Texas Facilities Commission, building security, and the agency mailroom personnel to determine the best way for high value assets to be delivered. Some ideas include: 1. Better signage. 2. Have a drop box placed so that packages can be delivered. 3. Allow security desk personnel to sign for packages, or escort delivery personnel to the Agency. 4. Update Purchase Orders to include instructions for vendor delivery personnel to contact the Agency to arrange for a drop-off time. This ensures that someone is onsite to accept the delivery. 5. Set a dollar amount for items that will require a signature at time of delivery.	Fully Addressed
4	February 2022	22-001 IT Asset Management	Not Rated	The Asset Management Guides, Instructions & Procedures (SOP) should be updated to reflect current processes and/or best practices.	1. Update Appendix C: Receiving Process to include the IT Department (ITD) and any new processes that are now occurring. These include but not limited to: a. Property Specialist delivering property to ITD. b. ITD updating Snipe-IT. c. ITD assigning the property to users.	Fully Addressed

DETAILED FINDINGS, RECOMMENDATIONS, AND IMPLEMENTATION STATUS

#	Audit Date	Audit # & Name	Risk Ranking	Finding	Recommendation	Status
4 Cont.	February 2022	22-001 IT Asset Management	Not Rated	The Asset Management Guides, Instructions & Procedures (SOP) should be updated to reflect current processes and/or best practices.	2. Whenever ITD is involved in the asset management process there should be procedures or Service Level Agreements (SLAs) created to indicate how long they have to complete data entry/notification to property management personnel. These should be very clear and concise. Some areas include: a. The respective property must be received in Snipe-IT within eight (8) hours of receipt from property management. b. Snipe-it must be updated within one (1) business day of issuing a device. c. Snipe-IT must be updated within one (1) business day of items being sent for repair. 3. Work with ITD to determine the dollar limit for consumable IT equipment. This will ensure the correct assets are tracked in Snipe-IT. 4. Create a well-defined process for leased item tracking in Snipe-IT. This should include the following at a minimum: a. Tracking of serial numbers, contract numbers, model numbers. These should be correlated to the lease end date. This is so that the equipment that was leased is what is returned at the end of the lease.	Fully Addressed

DETAILED FINDINGS, RECOMMENDATIONS, AND IMPLEMENTATION STATUS

#	Audit Date	Audit # & Name	Risk Ranking	Finding	Recommendation	Status
5	February 2022	22-001 IT Asset Management	Not Rated	While reviewing the Asset Management SOP it was found that the TREC SPA Accounting Procedures document has not been updated/reviewed since 2017.	Update the TREC SPA Accounting Procedures to match current processes. These include: a. Changes to Texas Administrative Code (TAC) Title 34, Rule 5.200 b. Changes to the Asset Management processes (Asset Management SOP)	Fully Addressed
6	February 2022	22-001 IT Asset Management	Not Rated	The Asset Management Guides, Instructions & Procedures (SOP) does not meet all of the requirements of the Texas Government Code 403 Subchapter L.	Update the SOP to address the missing controls of Government Code 403 Subchapter L: 1. Update Section VIII of the SOP in the event that TREC lends property to another agency. This will ensure a process exists in the event that the agency needs to loan assets to another agency. (403.273d) 2. Add a process for the changing of the agency head and/or property manager. This process should include the following: (404.274) a. The outgoing head of the agency or property manager shall complete the form required by the comptroller about property in the agency's possession. b. The outgoing head of the agency or property manager shall deliver the form to the incoming head of the agency or property manager. c. After verifying the information on and signing the form, the incoming head of the agency or property manager shall submit a copy of the form to the comptroller.	Fully Addressed

DETAILED FINDINGS, RECOMMENDATIONS, AND IMPLEMENTATION STATUS

#	Audit Date	Audit # & Name	Risk Ranking	Finding	Recommendation	Status
7	June 2024	24-001 Information Technology (Confidential Report)	Some Improvement Needed	The Information Technology policies designed to address TAC §202 security control standard requirements are in draft form and have not been formally adopted as policy. Additionally, we noted some security control standards were not addressed in those policies.	We agree with the finding and anticipate having all policies and procedures adopted and communicated to staff by June 28, 2024. We will increase our formal review and approval of security policies to be annual rather than every two years to be completed prior to the end of each calendar year. The IT security analyst will coordinate the review.	Fully Addressed
8	June 2024	Information Technology (Confidential Report)	Major Improvement Needed	The Business Continuity Plan does not effectively designate an official to manage the development, documentation, and dissemination of the contingency planning policy.	Update the Business Continuity Plan (BCP) to explicitly designate an individual (by job title) to manage the development, documentation, and dissemination of the contingency planning policy.	Fully Addressed

DETAILED FINDINGS, RECOMMENDATIONS, AND IMPLEMENTATION STATUS

#	Audit Date	Audit # & Name	Risk Ranking	Finding	Recommendation	Status
9	June 2024	Information Technology (Confidential Report)	Major Improvement Needed	The Business Continuity Plan has not been updated, reviewed, and approved since October 2014 and likely does not represent the current operating environment.	Review and update the BCP to ensure that the elements addressed throughout the document represent the current operating environment and address consideration of the various areas identified in contingency planning standards, such as TX DIR Security Control Standards Catalog.	Fully Addressed
10	June 2024	Information Technology (Confidential Report)	Major Improvement Needed	Business Continuity Plan testing has not been documented since 2014, increasing the risk of future business continuity failures.	Perform and document periodic BCP testing exercises to determine the effectiveness of the plan and the readiness to execute the plan.	In-Progress Target Completion Date: 10/31/2025

DETAILED FINDINGS, RECOMMENDATIONS, AND IMPLEMENTATION STATUS

#	Audit Date	Audit # & Name	Risk Ranking	Finding	Recommendation	Status
11	June 2024	Information Technology (Confidential Report)	Major Improvement Needed	The FY2023 vulnerability assessment report indicated results for web applications only and did not cover the full TREC environment. Specifically, the network ranges where workstations and servers reside were not scanned. Additionally, we found that the frequency of vulnerability scans did not ensure that vulnerabilities were identified and monitored when new vulnerabilities potentially affecting the system are identified and reported.	Establish a process for performing periodic vulnerability assessments across the whole environment. State implementation guidance for Security Control Standard RA-5 | Vulnerability Monitoring and Scanning indicates that the information system and all hosted applications should be scanned at least annually and when significant new vulnerabilities potentially affecting the system are identified and reported. Because critical security vulnerabilities are identified by system vendors, such as Microsoft on a monthly basis, we recommend implementing at least monthly scans.	Fully Addressed
12	June 2024	Vulnerability Scan Report	Not Rated	We conducted a vulnerability scan of the entire TREC IT environment which resulted in the identification of several issues. The results of these scans were provided to TREC IT management in a separate confidential report, found in the Vulnerability Scan Report.	Establish a process for performing periodic vulnerability assessments across the whole environment.	Fully Addressed