TEXAS REAL ESTATE COMMISSION

Internal Audit Services

AN INTERNAL AUDIT OF

Information Technology

Report No. 24-001

Public Version

June 6, 2024

Our full report contains information that is deemed to present potential risks related to public safety, security, or the disclosure of private or confidential data. As such, it is a restricted, confidential, report that is exempt from the requirements of the Texas Public Information Act under the provisions of Texas Government Code, Section 552.139. We prepared this summary report for public release when requested.

Report Highlights

Why Was This Review Conducted?

McConnell & Jones LLP (MJ) serving as the outsourced internal audit function (Internal Audit) for the Texas Real Estate Commission (TREC).

MJ performed this internal audit as part of the approved FY 2023 and FY 2024 Annual Internal Audit Plan.

Business Objectives and Scope

To ensure management's processes and controls are designed to:

- Comply with Texas Administrative Code (TAC) §202,
- Implement effective Cybersecurity Measures,
- Implement effective Continuity of Operations, and
- Effectively manage network and system vulnerabilities identified through vulnerability scanning.

The audit scope period was September 1, 2023 to May 15, 2024.

Audit Focus

The audit focused on the following Information Technology aspects:

- Information Technology policies and procedures,
- Cybersecurity measures,
- Continuity of operations planning processes, and
- Vulnerability management processes.

Our full report contains information that is deemed to present potential risks related to public safety, security, or the disclosure of private or confidential data. As such, it is a restricted, confidential, report that is exempt from the requirements of the Texas Public Information Act under the provisions of Texas Government Code, Section 552.139. We prepared this summary report for public release when requested.

Audit Conclusions

Overall, we noted that TREC's IT security technical controls are in place to protect the information resources, however, control weaknesses have been identified as documented throughout this report. Specifically:

- 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 security control standards that were not addressed in those policies.
- The Business Continuity Plan (BCP) does not effectively designate an official to manage Business Continuity.
- The BCP has not been updated, reviewed, or approved since October 2014.
- BCP testing has not been documented since 2014.
- Data removed from this public report due to the sensitive nature and risks associated with information technology security.

We identified 5 control weaknesses in the design of the IT program and 7 opportunities where the internal control or process is effective as designed but can be enhanced.

Internal Control Rating

Major Improvement Needed.

What Did We Recommend?

1. Complete and formally adopt the IT policies to address all security control standards. Then, ensure that the policy is reviewed and periodically updated.
2. Update the BCP to explicitly designate an individual (by job title) to manage Business Continuity.
3. Review and update the BCP, addressing all TX DIR Security Control Standards.
4. Perform and document periodic BCP testing exercises.
5. Data removed from this public report due to the sensitive nature and risks associated with information technology security.

Number of Findings by Residual Risk Rating

Category	High	Medium	Low	Total
Findings	2	3	0	5
Improvement Opportunities	7			

Introduction

We performed this audit as part of the approved FY 2024 Annual Internal Audit Plan. This audit was conducted in accordance 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 accomplishes that requirement.

Our full report contains information that is deemed to present potential risks related to public safety, security, or the disclosure of private or confidential data. As such, it is a restricted, confidential, report that is exempt from the requirements of the Texas Public Information Act under the provisions of Texas Government Code, Section 552.139. We prepared this summary report for public release when requested.

Business Objective, Conclusion, and Internal Control Rating

The purpose of this audit was to assess management's Information Technology (IT) program to ensure that processes and controls were designed to ensure:

- Compliance with Texas Administrative Code (TAC) §202,
- Implementation of effective Cybersecurity Measures,
- Implementation of effective Continuity of Operations, and
- Effective management of network and system vulnerabilities identified through vulnerability scanning.

The scope period was September 1, 2023 to April May 15, 2024.

This audit identified findings that resulted in an overall internal control rating of: **Major Improvement Needed.** **Exhibit 1** describes the internal control rating**.**

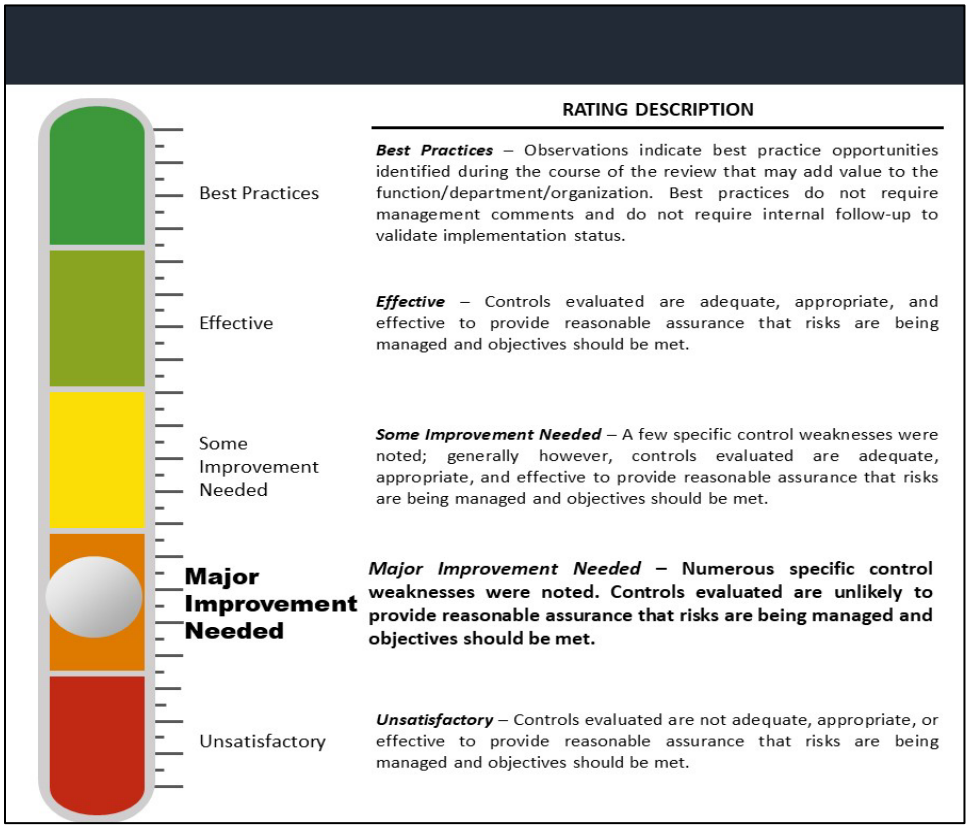

Exhibit 1: Internal control rating description.

Finding vs Improvement Opportunity

We define a finding as an internal control weakness or non-compliance with required policy, law, or regulation. We define an improvement opportunity as an area where the internal control or process is effective as designed but can be enhanced.

Findings and Risk Rating Summary

Inherent risk is the business risk associated with the respective function or process if internal controls were not in place or were not effective. Residual risk is Internal Audit's ranking of the remaining risk or likelihood of a negative event occurring with the internal processes and controls in place. **Exhibit 2** provides a summary of our audit observations. See the findings and management response section of this report for a discussion of all issues identified recommendations and management responses.

Business Objective / Focus Area	Business Risk Ranking	Control Effectiveness	Recommendations
1. Cybersecurity Measures	Inherent Risk: **High** Residual Risk: **Low**	**Generally Effective** **Opportunity for Improvement** **OFI-01** TREC does not automatically remove access to "stale accounts", that is, those accounts that have not logged in for a specified period (e.g. 90 days). This is an additional control to help catch exceptions that may occur in the termination process. **OFI-02** Manual user access reviews are performed on an annual basis.	***Opportunity for Improvement*** **OFI-01** As a best practice, TREC should consider implementing a scheduled script to check for and disable inactive accounts or add a step to the manual review process to specifically check for accounts where the last login date was greater than a defined time period (e.g., 90 days). **OFI-02** Perform user access reviews more frequently, such as on a quarterly basis.
2. Compliance with TAC §202	Inherent Risk: **High** Residual Risk: **High**	**Major Improvement Needed** (See Findings and Management Response Section Business Objective #2) **Finding** **24-001.01** 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.	**Finding** **24-001.01** Review and update the Information Technology policies to address all security control standards and submit them to executive leadership for review and approval. Then, publish the policies and disseminate them to all applicable personnel. Ensure that the policies are reviewed and approved on a periodic basis (at least annually) and

Business Objective / Focus Area	Business Risk Ranking	Control Effectiveness	Recommendations
			when significant changes are needed.
		Opportunity for Improvement **OFI-03** The *Information Technology - System and Services Acquisition Policy* contains two Developer Configuration Management sections. **OFI-04** The *Information Technology - System and Information Integrity Policy* section numbering resets to one at this section.	**Opportunity for Improvement** **OFI-03** Review and update the Information Technology - System and Services Acquisition Policy to eliminate duplicated content. **OFI-04** Review and update the Information Technology - System and Information Integrity Policy to appropriately sequence sections.
3. Continuity of Operations Plan	Inherent Risk: **High** Residual Risk: **High**	**Major Improvement Needed** (See Findings and Management Response Section Business Objective #3) **Findings** **24-001.02** The Business Continuity Plan does not effectively designate an official to manage the development, documentation, and dissemination of the contingency planning policy. **24-001.03** The Business Continuity Plan has not been updated, reviewed, and approved since October 2014 and likely does not represent the current operating environment. **24-001.04** Business Continuity Plan testing has not been documented since 2014, increasing the risk of future business continuity failures. **Opportunity for Improvement** **OFI-05** Although the BCP was designed to address elements now codified as standards by TAC §202 and the DIR Security	**Findings** **24-001.02** Update the Business Continuity Plan to explicitly designate an individual (by job title) to manage the development, documentation, and dissemination of the contingency planning policy. **24-001.03** Review and update the Business Continuity Plan 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. **24-001.04** Perform and document periodic testing exercises to determine the effectiveness of the plan and the readiness to execute the plan. **Opportunity for Improvement** **OFI-05** Update the BCP to acknowledge requirements to meet TAC §202 and other

Business Objective / Focus Area	Business Risk Ranking	Control Effectiveness	Recommendations
		Control Standards Catalog, there is no explicit statement of intent of alignment with those adopted standards. **OFI-06** The BCP does not prohibit unauthorized changes or classify the BCP as internal use only or confidential. Additionally, technical controls should be in place to ensure the BCP is protected from unauthorized changes. **OFI-07** The Business Continuity Plan does not address periodic employee training, which increases the likelihood of operational failures when disasters occur.	relevant regulatory requirements. **OFI-06** Update the BCP to prohibit unauthorized changes and classify the BCP as confidential or similar level of data classification. Additionally, ensure that "write" access to the BCP is enabled only for those individuals whose job responsibilities required BCP management. **OFI-07** Establish a periodic (at least annual) business continuity training program to ensure that employees are up to date with changing requirements and procedures.
4. Vulnerability Scan	Inherent Risk: **High** Residual Risk: **High**	**Major Improvement Needed** Data removed from this public report due to the sensitive nature and risks associated with information technology security. As such, it is a restricted, confidential, item that is exempt from the requirements of the Texas Public Information Act under the provisions of Texas Government Code, Section 552.139.	**Finding** **24-001.05** Data removed from this public report due to the sensitive nature and risks associated with information technology security. As such, it is a restricted, confidential, item that is exempt from the requirements of the Texas Public Information Act under the provisions of Texas Government Code, Section 552.139.

Exhibit 2: *Summary of Internal Audit Findings and Recommendations.*

Background

Texas Administrative Code (TAC) §202 establishes a baseline of information security responsibilities for state agencies and defines control requirements for those agencies in the Texas (TX) Department of Information Resources (DIR) Security Control Standards Catalog. TAC §202 also provides specific definitions for the roles and responsibilities of those charged with the protection of the agency's information resources, such as applications, systems, and data. These definitions can be found in TAC §202.1 Applicable Terms and Technologies for Information Security Standards.

As the Agency Head, the Executive Director is ultimately responsible for the agency's information resources. Included in these responsibilities are designating an Information Security Officer to administer information security controls to meet those requirements and allocating resources for the implementation of such controls. In compliance with these requirements, the Agency Head has appointed the Information Technology Director

as the designated Information Security Officer. As noted in the organizational chart depicted in **Exhibit 3** below, the Information Technology Director reports directly to the Executive Director.

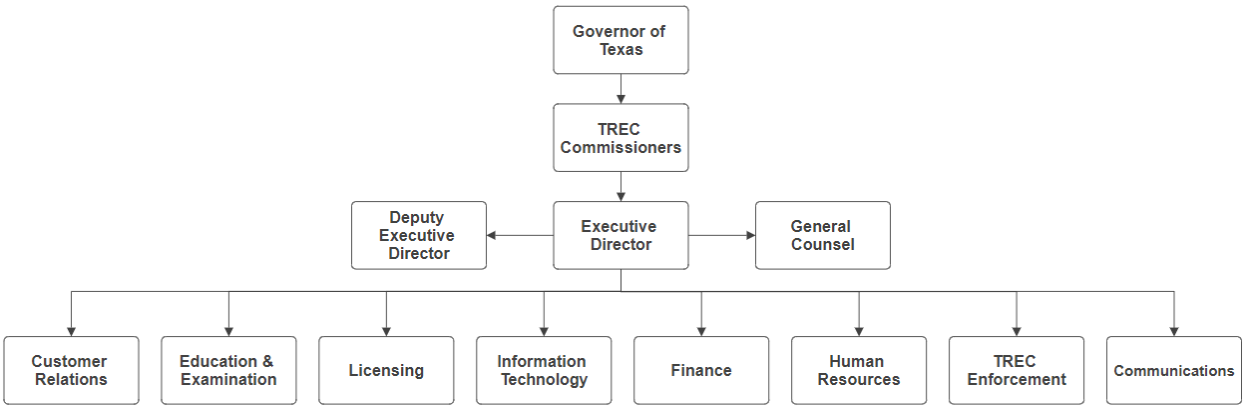

Exhibit 3: TREC Organizational Chart

In this role, the Information Technology Director works with Information Owners, Information Custodians, and Information Users to ensure that processes and controls are in place to protect the confidentiality, integrity, and availability of TREC's information resources. It is through these efforts that TREC intends to comply with TAC §202 requirements and mitigate cybersecurity risks to a level acceptable to the agency and its commissioners. Additionally, the Information Technology Director is responsible for overseeing the agency's vulnerability management program to ensure that system and application vulnerabilities are identified, analyzed, and remediated according to the associated risks.

As part of the TAC §202 requirements, the agency is also required to manage business continuity and disaster recovery, collectively referred to as contingency planning. The purpose of business continuity is to ensure that the organization can continue to perform its mission critical functions during an event that could potentially impact the agency's ability to meet its business objectives. The purpose of disaster recovery is to ensure that the organization is able to recover from an event that does cause a business disruption. In response to the increased need for organizations to react to large-scale business disruptions (such as the COVID-19 outbreak in 2020), our focus was to assess the organization's business continuity plan. It should be noted that the terms "Business Continuity" and "Continuity of Operations" are sometimes used interchangeably, where "Continuity of Operations" is traditionally favored by public and government entities. "Business Continuity" is traditionally favored by businesses and encompasses a broader scope, such as financial resilience and the ability to continue to process business transactions. Due to the nature of TREC/TALCB and TAC §202's use of the term "Continuity of Operations" and inconsistencies in TREC's documentation related to business continuity/continuity of operations, for the purpose of this review, both terms may be used to imply "Continuity of Operations."

The purpose of this audit is to assess the Information Technology program to ensure that processes and controls were designed to ensure:

- Compliance with Texas Administrative Code (TAC) §202,
- Implementation of effective Cybersecurity Measures,
- Implementation of effective Continuity of Operations, and
- Effective management of network and system vulnerabilities identified through vulnerability scanning.

Detailed Findings and Management Response

This section of the report provides a detailed discussion of opportunities we noted during the audit along with recommendations to improve internal controls or the business process.

Business Objective #1: Cybersecurity Measures

Business Risk Rating (Inherent): High

Business Risk Rating (Residual): Low

Business Objective: To ensure processes and controls are designed to implement cybersecurity measures to comply with regulatory requirements and reduce cybersecurity risk to an acceptable level.

Control Rating: Generally effective.

Finding Narrative:

The Information Security Officer works with Information Owners, Custodians, and Staff to develop policies and procedures to protect the agency's information resources. The Information Security Officer is also responsible for ensuring that staff are trained and that technical controls are in place and effective to protect the agency's information resources. The Information Security Officer reports directly to the Executive Director.

Our review of the technical controls in place determined that TREC's cybersecurity controls follow established cybersecurity standards and practices, such as secure account and password management, security patching and updates, and anti-malware protection. Please note, cybersecurity monitoring and vulnerability management are addressed separately in **Business Objective #4: Vulnerability Scanning**.

Criteria	➲ **Texas Administrative Code §202** ➲ **Texas Dept. of Information Resources Security Control Standards Catalog**
Effect/Risk/Impact	➲ Data breaches or operational disruptions caused by weak cybersecurity measures resulting in financial losses and reputational damage.
Control Tests	➲ Inquired of management. ➲ Observed technical controls in place, including two-factor authentication and periodic password update requirements. ➲ Inspected evidence of technical controls in place.
Management Controls in Place	➲ TREC has implemented technical system controls to protect from unauthorized access, unpatched system vulnerabilities, and malware.
Findings / Opportunities	**Opportunity for Improvement** ➲ **OFI-01** TREC does not automatically remove access accounts that have been inactive for an organization-defined time period. Additionally, the periodic user account review does not include removing access from accounts that have been inactive for an organization-defined time period. ➲ **OFI-02** Manual user access reviews are performed on an annual basis.
Root Cause	➲ Not applicable.

Recommended Actions:

Opportunity for Improvement

OFI-01 TREC should consider implementing a scheduled script to check for and disable inactive accounts or add a step to the manual review process to specifically check for accounts where the last login date was greater than a defined time period (i.e., 90 days).

OFI-02 Perform user access reviews more frequently, such as on a quarterly basis.

Management Response:

N/A – Management response is not needed for Opportunities for Improvement.

Business Objective #2: Compliance with TAC §202

Business Risk Rating (Inherent): High

Business Risk Rating (Residual): High

Business Objective: To ensure that processes and controls are in place to comply with TAC §202.

Control Rating: Major Improvement Needed

Finding Narrative:

In compliance with TAC §202, TREC's Executive Director is responsible for overseeing TREC's information security plan. TREC has designated an Information Security Officer responsible for developing and maintaining the information security plan based on risk assessments performed on a biennial basis.

The Information Security Officer, with support from Information Owners, Custodians, and Staff, is responsible for implementing policies and procedures in compliance with TAC §202 and the TX DIR Security Control Standards Catalog. To this end, policy and procedures have been drafted with explicit reference to TX DIR Security Control Standards. However, due to staffing changes and a lack of prioritization, the policies designed to comply with those standards are in draft form and do not fully address all relevant requirements.

Our review included comparing the existing draft policies with the TX DIR Security Control Standards to identify any gaps in coverage to facilitate the implementation of these policies.

Criteria	➲ **Texas Administrative Code §202** ➲ **Texas Dept. of Information Resources Security Control Standards Catalog**
Effect/Risk/Impact	➲ Non-compliance with TAC §202 and the underlying security controls defined in the Texas DIR Security Control Standards Catalog caused by a weak information technology program resulting in regulatory penalties and reputational damage.
Control Tests	➲ Inquired of management. ➲ Inspected policies and procedures.
Management Controls in Place	➲ TREC has assigned responsibility for the development of policies and procedures in compliance with TAC §202 requirements. ➲ TREC has drafted policies designed to comply with TAC §202 requirements.
Findings / Opportunities	**Finding** ➲ **24-001.01** 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. **Opportunities for Improvement** ➲ **OFI-03** The *Information Technology - System and Services Acquisition Policy* contains two Developer Configuration Management sections. ➲ **OFI-04** The *Information Technology - System and Information Integrity Policy* section numbering resets to one at this section.
Root Cause	➲ **24-001.01** Executive leadership has not prioritized the development, documentation, and dissemination of effective access control policies. Additionally, there have been staffing changes that have caused disruptions in the continuous management of the policy.

Recommended Actions:

Finding

24-001.01 Review and update the Information Technology policies to address all security control standards and submit them to executive leadership for review and approval. Then, publish the policies and disseminate them to all applicable personnel. Ensure that the policies are reviewed and approved on a periodic basis (at least annually) and when significant changes are made.

Opportunities for Improvement

OFI-03 Review and update the Information Technology - System and Services Acquisition Policy to eliminate duplicated content.

OFI-04 Review and update the Information Technology - System and Information Integrity Policy to appropriately sequence sections.

Management Response:

24001-01 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.

Business Objective #3: Continuity of Operations Planning

Business Risk Rating (Inherent): High

Business Risk Rating (Residual): High

Business Objective: To ensure processes and controls are designed to effectively address continuity of operations to comply with regulatory requirements and reduce contingency planning risk to an acceptable level.

Control Rating: Major Improvement Needed

Finding Narrative:

TREC developed and documented the *Business Continuity Plan for Texas Real Estate Commission and Texas Appraiser Licensing and Certification Board* (BCP) in 2014 to address continuity of operations. We noted that the content of the BCP addresses the majority of elements considered important to effective contingency planning, as defined by TX DIR Security Control Standards. However, due to changes in staff and unclear designation of authority for management of the BCP, the document has not been updated since 2014. As such, it is unlikely that the contents of the document represent TREC's current operating environment.

In 2021, responsibility for updating the plan has been informally assigned to the Human Resources Director. Since accepting this responsibility, the Human Resources Director has received FEMA business continuity training and has met with SORM (State Office of Risk Management) to gain an understanding of business continuity, disaster recovery, and general risk management. However, due to a lack of prior experience, inadequate support, and conflicting responsibilities, the BCP was never updated.

As noted above, we believe that the current BCP addresses most of the elements considered important to effective contingency planning and should serve as a solid foundation for developing a current BCP that addresses the elements recommended below.

Criteria	➲ **Texas Administrative Code §202** ➲ **Texas Dept. of Information Resources Security Control Standards Catalog**
Effect/Risk/Impact	➲ Weak controls over continuity of operations increases the likelihood and potential impact of operational failures during a business disruption.
Control Tests	➲ Inquired of the IT Director

	➲ Inquired of the Human Resources Director ➲ Reviewed the *Business Continuity Plan for Texas Real Estate Commission and Texas Appraiser Licensing and Certification Board*.
Management Controls in Place	➲ TREC has developed and documented a contingency plan that addresses the majority of elements required by the TX DIR Security Control Standards. ➲ TREC has informally designated the Human Resources Director as responsible for management of the BCP.
Findings / Opportunities	**Findings** ➲ **24-001.02** The Business Continuity Plan implies but does not explicitly designate an official to manage the development, documentation, and dissemination of the contingency planning policy. ➲ **24-001.03** The Business Continuity Plan has not been updated, reviewed, or approved since October 2014, which increases the likelihood that the BCP does not represent the current operating environment. ➲ **24-001.04** BCP testing has not been documented since 2014, increasing the risk of future business continuity failures. **Opportunities for Improvement** ➲ **OFI-05** Although the BCP was designed to address elements now codified as standards by TAC §202 and the DIR Security Control Standards Catalog, there is no explicit statement of intent of alignment with those adopted standards. ➲ **OFI-06** The BCP does not prohibit unauthorized changes or classify the BCP as internal use only or confidential. Additionally, technical controls should be in place to ensure the BCP is protected from unauthorized changes. ➲ **OFI-07** The Business Continuity Plan does not address periodic employee training, which increases the likelihood of operational failures when disasters occur.
Root Cause	**Findings** ➲ **24-001.02** The BCP was developed prior to significant staffing changes and transfer of authority was not clearly defined or executed. ➲ **24-001.03** The BCP does not explicitly designate an official to manage the development, documentation, and dissemination of the BCP. Additionally, the BCP does not address transfer of authority over management of the BCP. ➲ **24-001.04** The BCP does not explicitly designate an official to manage the development, documentation, and dissemination of the BCP. Additionally, the BCP does not address transfer of authority over management of the BCP.

Recommended Actions:

Findings

24-001.02 Update the Business Continuity Plan to explicitly designate an individual (by job title) to manage the development, documentation, and dissemination of the contingency planning policy.

24-001.03 Review and update the Business Continuity Plan 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.

24-001.04 Perform and document periodic testing exercises to determine the effectiveness of the plan and the readiness to execute the plan.

Opportunities for Improvement

OFI-05 Update the BCP to acknowledge requirements to meet TAC §202 and other relevant regulatory requirements.

OFI-06 Update the BCP to prohibit unauthorized changes and classify the BCP as confidential or similar level of data classification. Additionally, ensure that write access to the BCP is enabled only for those individuals whose job responsibilities required BCP management.

OFI-07 Establish a periodic (at least annual) business continuity training program to ensure that employees are up to date with changing requirements and procedures.

Management Response:

24-001.02 Management acknowledges this finding. We are revising the Continuity of Operations Plan to include: 1) Action plan to review and address the plan on an annual basis, 2) Identify the owner of the plan, and 3) Timeline for completion will be October 2024.

24-001.03 Management acknowledges this finding. The plan is currently being revised. Completion is scheduled for October 2024.

24-001.04 Management acknowledges this finding. A schedule will be included in the plan to test it on an annual basis.

Business Objective #4: Vulnerability Scan

Business Risk Rating (Inherent): High

Business Risk Rating (Residual): High

Business Objective: To ensure processes and controls are designed to effectively manage system vulnerabilities to comply with regulatory requirements and reduce vulnerability management risk to an acceptable level.

Control Rating: Major Improvement Needed

Finding Narrative:

Data and tables removed from this public report due to the sensitive nature and risks associated with information technology security. As such, it is a restricted, confidential, item that is exempt from the requirements of the Texas Public Information Act under the provisions of Texas Government Code, Section 552.139.

Recommended Actions:

24-001.05 Data removed from this public report due to the sensitive nature and risks associated with information technology security. As such, it is a restricted, confidential, item that is exempt from the requirements of the Texas Public Information Act under the provisions of Texas Government Code, Section 552.139.

Management Response:

24-001.05 Data removed from this public report due to the sensitive nature and risks associated with information technology security. As such, it is a restricted, confidential, item that is exempt from the requirements of the Texas Public Information Act under the provisions of Texas Government Code, Section 552.139.

LIST OF APPENDICES

Due to the form and high-level information provided as appendices, separate digital files have been provided to management.

List of appendices removed from this public report due to the sensitive nature and risks associated with information technology security. As such, it is a restricted, confidential, item that is exempt from the requirements of the Texas Public Information Act under the provisions of Texas Government Code, Section 552.139.