Public Utility Commission of Texas

Electricity • Telecommunications • Water & Sewer

Audit on the Information Technology Division's Compliance with Select Information Security Standards

Project #2024.05
Report Date: May 2024

1701 N. Congress Ave
P.O. Box 13326
Austin, TX 78711-3326

512-936-7000
info@puc.texas.gov
puc.texas.gov

Executive Summary

We reviewed processes and controls over the Information Technology Division's compliance with information security standards for fiscal year 2023 (September 1, 2022, to August 31, 2023). The primary objective of the audit was to evaluate the processes and controls in place to ensure compliance with select Texas Administrative Code Title 1, Part 10, Chapter 202 Subchapter B (TAC 202), Information Security Standards for State Agencies and assess the adequacy and effectiveness of policies and procedures.

The audit focused on (a) roles and responsibilities for the agency head, information security officer, and other key personnel, (b) risk assessment and management, (c) security controls and standards, (d) incident response and reporting, (e) continuity of operations plan and disaster recovery plan, (f) security awareness and training, and (g) third-party and cloud service provider management.

Overall, we found that processes and controls have been established to provide assurance that the agency complies with the following TAC 202 requirements as it relates to:

- Providing security awareness training to new employees during the agency's onboarding process.
- Providing ongoing information security awareness training annually to all users to continuously protect the agency's information resources.
- Developing and implementing some information technology policies to protect the agencies data.
- Designating a data management officer.
- Designating an Information Security Officer (ISO) who is a Certified information Systems Security Professional (CISSP), possess the education and training to manage information security requirements, and understands the agency's mission and processes.
- Developing and submitting an agency-wide information security plan to the Department of Information Resources (DIR) in a timely manner.
- Ensuring that third-party service providers are TX-RAMP certified prior to providing cloud services to the agency.

However, we also identified processes for improvement.

To minimize security risk, those processes for improvement and the Detailed Results Section of this report, were omitted from public disclosure due to its confidential and sensitive nature, and communicated to the Commission and management in writing, in accordance with Section 9.61 of the U.S. Government Accountability Office's Generally Accepted Government Auditing Standards. Under the provisions of Texas Government Code, Section 552.139, the omitted information is also exempt from the requirements of the Texas Public Information Act.

Background

The Public Utility Commission of Texas is the state agency responsible for economic regulation of Texas' electric, telecommunication, and water and wastewater utilities.

The agency oversees the state's competitive utility markets, regulates rates and services, and enforces rules to protect consumers and promote reliable, high-quality infrastructure. Through effective

oversight, rate regulation, and consumer assistance, the agency ensures consumers across the state are treated fairly and receive the economic and reliability benefits of competition.

The agency is led by five full-time Commissioners who are appointed by the Governor and confirmed by the Texas Senate for six-year terms with one commissioner serving as the Chairman. The commissioners select an executive director to manage the agency's staff and daily operations. The agency professional staff include generalists and specialists with experience in engineering, economics, law, finance, security and risk management, and public and government affairs.

The Information Technology division provides support for the technological needs of the agency commissioners, executive management, and agency staff members. These technological needs encompass the management of the agency's internal business systems, computing infrastructure, and information security program. The 15 member staff are organized into three groups: Operations Support, Application Development, and Data & Records Management.

The Operations Support team supports the agency desktop environment by installing, maintaining, and troubleshooting workstation software and hardware, and optimizing staff's ability to use their computer resources. Additionally, they manage the agency's servers, perform systems management and integration, support resolving IT related issues for staff, and oversee the planning, implementation, and monitoring of security measures for the protection of information systems and infrastructure.

The Application Development team creates and maintains support for over various internal and external business applications, provide application support to agency staff and external customers, databases administration, and perform business analysis and project coordination.

The Data & Records Management Team ensures agency compliance with the State Records Management Laws by overseeing the preparation and maintenance of the agency records retention schedule, the approval of all records transferred to the State Records Center and all requests to dispose of state records. They also protect records from inappropriate and unauthorized access and provide continuity in the event of a disaster.

Texas Government Code, Chapter 2054, Subchapter A, §2054.051 grants the Texas Department of Information Resources (DIR) amongst other things, the authority to provide leadership in and coordination of information resources management within state government and develop and publish policies, procedures, and standards relating to information resources management by state agencies. Also, §2054.052 states that DIR may adopt rules as necessary to implement its responsibility under this chapter. DIR established information security standards which are found in the Texas Administrative Code Title 1, Part 10, Chapter 202 Subchapter B (TAC 202). TAC §202.24(a) requires all state agencies to have an agency-wide information security program consistent with these standards. Each state agency should apply the security standards based on documented security risk management decisions. In addition, DIR has implemented a Security Control Standards Catalog, Version 2.1, based on the National Institute of Standards and Technology (NIST), Special Publication 800-53 as a requirement for TAC 202 compliance. TAC 202 audits are required at least every two years to ensure that all state agencies comply.

Objective

The overall objective of this audit is to evaluate the processes and controls in place to ensure compliance with select Texas Administrative Code Title 1, Part 10, Chapter 202 Subchapter B (TAC 202), Information Security Standards for State Agencies and assess the adequacy and effectiveness of policies and procedures.

Scope and Methodology

The scope of the audit is fiscal year 2023 (September 1, 2022, to August 31, 2023) and any other related periods.

The methodology for the audit consisted of a review of the following information:

- Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter B.
- Texas Government Code, Chapter 2054.
- Senate Bill (SB) 475.
- DIR's Cybersecurity Framework Control Objectives and Definitions.
- DIR's Security Control Standards Catalog.
- DIR's Data Classification Guide.
- Agency Information Technology Policies and Procedures.
- Systems / Applications inventory data.

Tests and procedures included the following:

- Reviewed agency policies and procedures, assessments, and related reports.
- Reviewed applicable statutes, laws, rules and requirements, information security standards and guidance.
- Examined supporting documentation to determine whether processes and controls were operating as designed.
- Interviewed management and staff.

Our audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* and the *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 audit findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our audit observations and conclusions based on our audit objective.

<u>Audit Team</u>
Nicky Carter, Director for Internal Audit
Barbette Mays, Senior Auditor

Detailed Results

To minimize security risk, the Detailed Results Section of this report, was omitted from public disclosure due to its confidential and sensitive nature, and communicated to the Commission and management in writing, in accordance with Section 9.61 of the U.S. Government Accountability Office's Generally Accepted Government Auditing Standards. Under the provisions of Texas Government Code, Section 552.139, the omitted information is also exempt from the requirements of the Texas Public Information Act.

Acknowledgements

The Internal Audit Division appreciates the assistance and cooperation provided to us by management and staff of the agency during this audit. For questions or additional information concerning this report, please contact Nicky Carter at 512-936-7432.

Distribution List

Public Utility Commission of Texas

Commissioners' Offices

Thomas J. Gleeson, Chairman
Krista Duke, Chief of Staff to Chairman Gleeson
Kathleen Jackson, Commissioner
Jennifer White, Chief of Staff to Commissioner Jackson
Lori Cobos, Commissioner
Jon Oliver, Chief of Staff to Commissioner Cobos
Jimmy Glotfelty, Commissioner
V.A. Stephens, Chief of Staff to Commissioner Glotfelty

Executive Director's Office

Connie Corona, Executive Director
Barksdale English, Deputy Executive Director

Program Area

Hayley Hall, Chief Operating Officer
Nathan Lilie, Information Technology Director (IRM)
Parrish Pratt, Information Security Officer
Brady Cox, Data & Records Management Officer
Chuck Bondurant, Director for Critical Infrastructure Security & Risk Management
Erica Gutierrez, Cybersecurity Policy Analyst

External Distribution

Legislative Budget Board
Governor's Office of Budget, Planning, and Policy
State Auditor's Office