



Review of Select Cybersecurity Processes Phase III: Texas Geographic Information Office (TxGIO)

Project #2024.06
July 2025

Executive Summary

The objective of the audit was to evaluate whether Texas Geographic Information Office (TxGIO)¹ applications, software, and databases complied with select agency Information Technology (IT) information security policies, state and federal information security standards, and relevant laws, rules, and regulations. We also considered opportunities to improve coordination between the organizational areas of IT and TxGIO.

The scope of the audit covered fiscal year 2024 through the first two quarters of fiscal year 2025, and other related periods, as necessary, for testing purposes. The review focused on processes and controls relating to the following: system development life cycle, project management², change management, incident response, use of open-source tools, and administrative and special access accounts.

Overall, our review found that TxGIO processes provided assurance that applications, software, and databases complied with IT's information security policies pertaining to change management, the use of open-source tools, and incident response. However, we also identified areas where improvements should be made to strengthen TxGIO's compliance with IT's information security policies pertaining to administrative and special access accounts, system development life cycle, and project management.

Prior to the audit, TxGIO began implementing several improvements to their procedures to better align and comply with IT's information policies and procedures in some of the areas included within this review. Following such policies and procedures, and implementing the recommendations provided in the Results section of this report will facilitate discussion and improve coordination between the two organizational areas.

To minimize security risks, details about the audit were communicated separately to management, Executive Administration, and the Board in a confidential report. Auditors provided recommendations to address the issues identified during this audit. Management agreed and provided their responses and the estimated implementation dates for each of the recommendations.

Pursuant to Standard 9.61 of the U.S. Government Accountability Office's Government Auditing Standards, certain information was omitted from this document because that information was deemed to present potential risks related to public safety, security, or the disclosure of private or confidential data. 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.

Objectives, Scope, and Methodology

Objective

The objective of the audit was to evaluate whether TxGIO applications, software, and databases comply with select agency IT information security policies, state and federal information security standards, and relevant laws, rules, or regulations. The review also considered opportunities to improve coordination between the organizational areas of IT and TxGIO.

¹ In 2023, the 88th Texas Legislature officially renamed Texas Natural Resources Information System (TNRIS) to the Texas Geographic Information Office.

² Project Delivery.

Scope and Methodology

The scope of the audit covered fiscal year 2024 (September 1, 2023, to August 31, 2024) and the first two quarters of fiscal year 2025 (September 1, 2024, to February 28, 2025), as well as any other related periods, and focused primarily on processes and controls relating to system development life cycle, project management, change management, and incident response, including the use of open-source tools and administrative and special access accounts.

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

- Texas Government Code, Chapter 2054.
- Title 1, Texas Administrative Code, Chapter 202.
- Title 1, Texas Administrative Code, Chapter 216.
- TWDB Information Technology (IT) Policies and Procedures:
 - Administrative and Special Access Policy.
 - Project Management and Project Request Governance Policy.
 - System Development Policy.
- Department of Information Resources (DIR) guidance:
 - DIR's Security Control Standards Catalog.
 - DIR's Cybersecurity Framework Control Objectives and Definitions.
 - DIR's Project Management (PM) Essentials (PM Lite).

Tests and procedures included the following:

- Interviewed management and staff.
- Reviewed applicable statutes, rules, laws, and requirements.
- Reviewed agency policies and procedures.
- Examined and tested support documentation pertaining to system development life cycle, project management, change management, and incident response.
- Assessed compliance with open-source software request and approval.

This engagement was conducted in accordance with the *Generally Accepted Government Auditing Standards* (GAGAS) and the *International Standards for the Professional Practice of Internal Auditing*. The Division followed the GAGAS unconditional requirements, documented justification for a pro tem departure from one applicable presumptively mandatory requirement pertaining to the external peer review, and achieved the objective of that requirement through other compensating means until met. Additionally, the standards require that we plan and perform the audit engagement to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our observations and conclusions based on our audit objectives.

The audit team consisted of:

David Ramos
Kim Thiel, CISA
Nicole Campbell, CIA, CISA

Closing

We would like to express our appreciation to management and personnel for their cooperation and assistance provided to the internal audit staff during this review. For questions or additional information concerning this report, please contact Nicole Campbell at (512) 463-7978.

Report Distribution

Internal Distribution

This confidential report was distributed internally to the following:

Board's Office

L'Oreal Stepney, P.E., Chairwoman
Kerry Niemann, Chief of Staff to Chairwoman L'Oreal Stepney, P.E.
Tonya R. Miller, Board Member
Ron Ellis, Chief of Staff to Board Member Tonya R. Miller

Executive Administrator's Office

Bryan McMath, Executive Administrator
Kathleen Ligon, Assistant Executive Administrator

Program Area

Richard Wade, Deputy Executive Administrator, Texas Geographic Information Office
Edna Jackson, Deputy Executive Administrator, Operations & Administration
Patricia Avitia, Chief Information Officer (CIO), Director of Information Technology
Joe Sepulveda, Deputy CIO, Assistant Director of Information Technology
Angela Gower, Information Security Officer

External Distribution

A redacted version of this confidential report was provided to the following:

Legislative Budget Board

audit@lbb.texas.gov

Governor's Office of Budget, Planning, and Policy

budgetandpolicyreports@gov.texas.gov

State Auditor's Office

iacoordinator@sao.texas.gov