Internal Audit Annual Report for FY 2025

TEXAS CIVIL COMMITMENT OFFICE

MARSHA MCLANE
EXECUTIVE DIRECTOR

I. Compliance with Posting Requirements

Texas Government Code, Section 2102.015 requires state agencies, as defined in the statute, to post certain information on Internet Web sites. The Texas Civil Commitment Office's Internal Audit will adhere to the following procedures to ensure compliance with posting requirements.

Texas Government Code, Section 2102.015(b) (1) requires posting of the agency's approved internal audit plan within 30-days of approval. In accordance with Texas Government Code, Section 2102.008, the annual audit plan developed by the internal auditor must be approved by the state agency's governing board.

The Fiscal Year 2026 Internal Audit Plan was presented to the Board of the Texas Civil Commitment Office at the August 15, 2025 meeting for Board approval and was approved by the Board on that date. The plan was submitted to web services for posting to the agency's website on August 15, 2025.

Texas Government Code, Section 2102.015(b) (2) requires posting of the agency's Internal Audit Annual Report. Texas Government Code, Section 2102.009 requires the internal auditor to prepare an annual report and submit the report before November 1 of each year to the governor, the Legislative Budget Board, the Sunset Advisory Commission, the state auditor, the state agency's governing board, and the administrator. The state auditor prescribes the form and content of the report, subject to the approval of the legislative audit committee.

This annual report was submitted to the agency's executive administration and will be submitted to the Board of the Texas Civil Commitment Office. The report will be posted to the agency's website.

Texas Government Code, Sections 2102.015(d) and (e) requires agencies to update the posting with:

- A detailed summary of the weaknesses, deficiencies, wrongdoings, or other concerns raised by the audit plan or annual report; and,
- A summary of the action taken by the agency to address concerns, if any, that are raised by the audit plan or annual report.

Any weaknesses, deficiencies, wrongdoings, or others concerns, if noted, will be posted as required.

II. Internal Audit for Fiscal Year 2025

Audit Report on Physical Security of Electronic Devices and Data Management Practices

The scope of this audit included the following key areas and processes:

- Policy Review
- Physical Security
- Data Access
- Data Backup and Recovery

These areas were evaluated using documentation and activities spanning the period from September 2024 through July 2025. A representative sample of items was selected to ensure coverage across all relevant activities.

Audit fieldwork was conducted between May 2025 and July 2025. The procedures performed were sufficient in scope and depth to support the conclusions presented in this report, and were designed to provide reasonable assurance regarding the effectiveness of controls within the audited areas.

Policy Review

The objective of this audit was to assess the organization's existing security policies and procedures to determine whether they are current, comprehensive, and aligned with both organizational goals and applicable regulatory requirements. The evaluation focused on identifying gaps, ensuring relevance to evolving security standards, and confirming that the policies support the organization's overall risk management framework.

Internal Audit obtained and reviewed the organization's policies, procedures, and standards related to information security to assess their adequacy and alignment with best practices. Training records were verified to confirm that employees had received instruction on applicable security protocols. Additionally, interviews were conducted with selected staff members to evaluate their understanding and practical application of the established security procedures.

Audit Conclusion & Recommendation

The results of the testing indicate that the current security protocols are both effective and consistently followed. Based on the procedures performed, the IT framework and associated controls appear to be in alignment with the core principles and requirements outlined in ISO/IEC 27001. This suggests a strong commitment to maintaining a secure and compliant information security environment.

Recommendation — The Safety of Client Records and Records Retention policy was last updated on April 15, 2016. Given the evolving nature of cybersecurity threats and best practices, it is recommended that this policy be reviewed and updated on a regular basis. Cybersecurity policies should be treated as living documents—subject to ongoing evaluation and revision to ensure

continued relevance, effectiveness, and alignment with current regulatory requirements and organizational needs.

Physical Security Audit

The objective of this audit was to evaluate the effectiveness of physical security measures, including facility access controls and hardware protection protocols.

Internal Audit conducted a comprehensive walk-through of the facility to assess its layout, existing security defenses, and potential vulnerabilities. Specific procedures included:

- Evaluation of entry and exit points, access control systems (e.g., badge readers, surveillance cameras), and visitor management processes.
- Observation of daily operations to verify adherence to established security protocols.
- Verification of asset inventory by performing both "floor-to-book" and "book-to-floor" comparisons, ensuring physical assets matched inventory records and vice versa.

Audit Conclusion & Recommendation

Testing results indicate that physical security barriers are in good condition and functioning as intended. Access controls are effectively implemented to restrict entry to sensitive areas, such as the Intermediate Distribution Frame (IDF) room, to authorized personnel only. The Asset Inventory Listing appears complete, accurate, and current. Additionally, procedures for issuing and returning electronic devices are well-defined and properly followed.

Recommendation — Internal Audit recommends updating the AM01 Asset Management Form to include accessories—such as keyboards and other peripherals—that are typically distributed with electronic devices. Maintaining a comprehensive and accurate asset inventory is a foundational element of effective cybersecurity. A complete inventory enables the organization to better understand its asset landscape, assess potential risks, and implement appropriate safeguards to protect sensitive information and infrastructure.

Data Access Audit

The objective of this audit was to evaluate the effectiveness of access controls to data, data encryption practices, and the security of data storage locations.

Internal Audit confirmed that the electronic devices selected for testing were password-protected and encrypted using BitLocker, with an additional BitLocker PIN required prior to accessing the operating system or any data stored on the hard drive. A review of job responsibilities and system access was conducted for a sample of employees to ensure that access privileges were appropriate and aligned with their roles. Access to systems was verified against assigned responsibilities to confirm proper authorization and segregation of duties.

Audit Conclusion & Recommendation

Testing results indicate that the organization's data and information assets appear secure. Access to data storage areas is restricted to authorized personnel, and electronic devices are protected through password authentication and full-disk encryption using BitLocker, with an additional PIN required for access.

Access controls are appropriately configured based on user roles and responsibilities, and procedures for issuing and returning access credentials are well-defined and consistently followed. Additionally, log management and analysis tools are in place to monitor system and application logs for anomalies and potential security incidents. However, documentation to support the completion of log reviews is not maintained, which may limit the ability to demonstrate oversight and accountability.

Recommendation — On a monthly basis, the Deputy Director reviews an access report for Corrections Software Solutions (CSS) to ensure that users maintain appropriate access to client information. Internal Audit recommends extending this practice to include other significant systems and applications. Regular audits of user access rights are a critical component of a robust cybersecurity framework, helping to ensure that access privileges remain aligned with employees' current roles and responsibilities.

Additionally, Internal Audit recommends securely retaining log data for a sufficient duration to mitigate risks associated with advanced persistent threats, which may remain undetected for extended periods. Logs should be reviewed periodically, and evidence of these reviews should be documented and maintained to support accountability and demonstrate effective oversight.

Data Backup & Recovery Audit

The objective of this audit was to assess the organization's data handling procedures, including data retention and disposal practices, system and software updates, data backup protocols, incident response readiness, and business continuity planning.

Internal Audit reviewed the organization's data retention policies to evaluate alignment with applicable requirements. The audit verified that systems and software on selected electronic devices were current and up-to-date. Real-time protection mechanisms were observed, and scan logs were reviewed for a sample of detected issues to assess threat monitoring practices.

Audit Conclusion & Recommendation

Testing results indicate that the organization's data retention policy aligns with applicable requirements. Software and systems were found to be current and up-to-date, and threat monitoring practices are in place and functioning effectively. However, Internal Audit was informed by the IT Administrator that Texas Civil Commitment Office does not directly manage data backups for the servers currently in use. Backup and recovery responsibilities are handled by third-party providers (e.g., Microsoft and CSS). As a result, Internal Audit was unable to independently verify the functionality of backup systems or confirm the organization's ability to restore data in the event

of an incident. Additionally, there is no documented Incident Response Plan (IRP) in place. The absence of a formal IRP may hinder the organization's ability to respond promptly and effectively to cybersecurity incidents or operational disruptions.

Recommendation — Internal Audit recommends developing a formal reporting and review process with Microsoft and Corrections Software Solutions (CSS) to ensure that Texas Civil Commitment Office is promptly informed of any potential threats to data availability. This proactive approach will enhance visibility into third-party data management practices and support timely risk mitigation.

Internal Audit recommends creating a comprehensive Business Continuity Plan (BCP) to strengthen organizational resilience. A well-defined BCP minimizes the impact of operational disruptions and ensures that critical business functions can continue or be restored quickly in the event of a failure. This is a vital component of an effective risk management and cybersecurity strategy.

III. Consulting Services and Other Activities

No consulting services or other activities were performed in Fiscal Year 2025.

IV. External Audit Services

No external audit services were procured in Fiscal Year 2025.

V. External Quality Assurance Review (Peer Review)

No external quality assurance reviews were performed in Fiscal Year 2025.

VI. Internal Audit Plan for Fiscal Year 2026

Budget – 200 Hours

The Texas Civil Commitment Office Internal Audit Plan for Fiscal Year 2026 will revisit and perform follow up of the FY 2024 Internal Audit of the SVP client funds. The scope of the audit work will include:

- Review reconciliation of the Base Balance Report to the Client SVP Bank Statement
- Review to ensure disbursements from SVP client fund accounts were properly authorized
- Review to ensure clients are informed of the balance in their accounts on a timely basis

- Review to determine if clients have an opportunity to question their account balance and acknowledge this via their signature.

Follow Up and Required Projects

- Fiscal Year 2025 Annual Report to State Leadership
- Fiscal Year 2026 Annual Risk Assessment
- Planning for the Fiscal Year 2027 External Peer Review
- General Administration

Texas Civil Commitment Office Internal Audit anticipates successfully completing the objectives outlined in the 2026 audit plan within the allocated 200 hours. Should the scope of beneficial audit activities expand beyond the original plan and potentially exceed the 200-hour threshold, a formal request for additional hours will be submitted to the Audit Committee prior to initiating work beyond the authorized limit.

Risk Assessment

The role of Internal Auditor was accepted by the undersigned on April 4, 2025. To gain an understanding of the risk environment within the Texas Civil Commitment Office, Internal Audit relied on the FY 2024 Annual Risk Assessment and held transition discussions with the previous Internal Auditor.

Looking ahead, Internal Audit recommends prioritizing a follow-up review of the recommendations and concerns identified in the prior audit of the Sexually Violent Predator (SVP) client funds. This review will help ensure that previously raised issues have been appropriately addressed and that corrective actions have been effectively implemented.

In preparation for the FY 2026 Annual Risk Assessment, Internal Audit will work closely with Texas Civil Commitment Office management to ensure the assessment accurately reflects any changes in the organization’s risk environment that may not have been captured in the FY 2024 Risk Assessment.

VII. Reporting Suspected Fraud and Abuse

Fraud Reporting: Article IX, Section 7.09, the General Appropriations Act (89th Legislature, Conference Committee Report)

This section of the Appropriations Act states:

Sec. 7.09. Fraud Reporting. A state agency or institution of higher education appropriated funds by this Act, shall use appropriated funds to assist with the detection and reporting of fraud involving state funds as follows:

(1) Providing information on the home page of the entity's website on how to report suspected fraud, waste, and abuse involving state resources directly to the State Auditor's Office. This

shall include, at a minimum, the State Auditor's Office fraud hotline information and a link to the State Auditor's Office website for fraud reporting; and

To implement (1) of Section 7.09, the Texas Civil Commitment Office has included a link on the Texas Civil Commitment Office website to the State Auditor's Fraud Reporting hotline.

(2) Including in the agency or institution's policies information on how to report suspected fraud involving state monies to the State Auditor's Office.

To implement (2) of Section 7.09, the Texas Civil Commitment Office has included in Policy 1.10, Texas Civil Commitment Office Ethics Policy, section II.B, which provides instructions for employees to report any conduct he or she believes to be in violation of the ethics policy to the Executive Director or Executive Director's designee, and to report suspected fraud, waste, or abuse involving state funds to the State Auditor's Office via phone to the State Auditor's Office Fraud Hotline 1-800-TX-AUDIT or online at https://sao.fraud.texas.gov/ReportFraud/.

Texas Government Code, Section 321.022.

This section of the Texas Government Code states:

COORDINATION OF INVESTIGATIONS.

(a) If the administrative head of a department or entity that is subject to audit by the state auditor has reasonable cause to believe that money received from the state by the department or entity or by a client or contractor of the department or entity may have been lost, misappropriated, or misused, or that other fraudulent or unlawful conduct has occurred in relation to the operation of the department or entity, the administrative head shall report the reason and basis for the belief to the state auditor. The state auditor may investigate the report or may monitor any investigation conducted by the department or entity.

(b) The state auditor, in consultation with state agencies and institutions, shall prescribe the form, content, and timing of a report required by this section.

(c) All records of a communication by or to the state auditor relating to a report to the state auditor under Subsection (a) are audit working papers of the state auditor.

To implement this statute, Policy 1.10, Texas Civil Commitment Office Ethics Policy, section II.C requires the Executive Director to report the reason and basis for any suspected misuse of state monies to the state auditor. As of the date of this report, the Texas Civil Commitment Office has not received any reports of loss, fraud, misuse, or other fraudulent of unlawful activities.