# STATE BAR OF TEXAS

# Internal Audit Services

AN INTERNAL AUDIT OF

# Information Technology & Cybersecurity

Public Report No. 25-003

March 28, 2025

McConnell Jones

Diverse Thinking | Unique Perspectives

*This report provides management with information about the condition of risks and internal controls at a specific point in time. Future changes in environmental factors and actions by personnel may impact the risks and internal controls in ways that this report cannot anticipate.*

## *Why Was This Review Conducted?*

McConnell & Jones LLP (MJ) serving as the outsourced internal audit function (Internal Audit) for the State Bar of Texas (SBOT) performed this internal audit as part of the approved FY 2025 Annual Internal Audit Plan.

## *Business Objectives and Scope*

To ensure confidentiality, integrity, and availability of information through:

- Security policy administration;
- A comprehensive security plan content and regular updates;
- Data protection through processes, tools, and systems;
- A documented incident response plan;
- Change management process including patch management processes; and
- Software vendor Service Organization Controls (SOC) monitoring and management.

The audit scope period was June 1, 2024 to January 31, 2025.

## *Audit Focus*

1. Did SBOT address prior audit findings and are information technology policies comprehensive and enforced to protect the organization?
2. Does SBOT's security plan address, and align with, key risk areas of SBOT's IT environment?
3. Does SBOT's IT processes, tools and systems protect confidential and sensitive data?
4. Are processes in place that would allow SBOT to quickly respond to an incident that compromised confidential and sensitive data?
5. Is an effective patch management program in place?
6. Does SBOT require software vendors to submit their Service Organization Control (SOC) reports on an annual basis?
7. Are the submitted SOC reports reviewed for internal control findings?
8. Does SBOT have processes in place to ensure that controls identified as their responsibility in vendor software SOC reports are monitored and addressed?

## *Audit Conclusions*

Our review of SBOT's internal control policies and procedures over Information Technology & Cybersecurity was based on the National Institute of Standards and Technology (NIST) Cybersecurity Maturity Model. We identified a few areas for improvement in order to attain the organization's preferred level of maturity for all cybersecurity risk management practices (Identify, Protect, Detect, Respond and Recover).

## *What Did We Recommend?*

We provided SBOT with recommendations to attain the organization's preferred level of maturity of the NIST Cyber Security Maturity Model.

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.

*We wish to thank all employees for their openness and cooperation. Without this, we would not have been able to complete our review.*

## Introduction

We performed this audit as part of the approved FY 2025 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 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

To ensure confidentiality, integrity, and availability of information through:

- Security policy administration;
- A comprehensive security plan content and updates;
- Data protection through processes, tools, and systems;
- Documented incident response processes;
- Change management processes including patch management processes; and
- Software vendor Service Organization Controls (SOC) monitoring and management.

The audit scope period was June 1, 2024 to January 31, 2025.

## 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 internal controls or processes are effective as designed but can be enhanced. A control weakness is a failure in the implementation or performance of internal controls. A control gap occurs when controls do not exist, do not effectively mitigate a risk, or are not operating effectively.

## 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 controls and processes in place.

## Background

The SBOT (State Bar of Texas) Information Technology (IT) Division is responsible for managing and securing the IT environment of the State Bar of Texas. Their key activities include conducting periodic IT risk assessments, developing and maintaining security plans, protecting confidential and sensitive data, and managing third-party software vendor relationships. The IT Division is also responsible for establishing policies and procedures for IT operations and information security.

When determining the maturity level of the organization's cybersecurity program, we referred to the National Institute of Standards and Technology (NIST), a U.S. government agency that helps businesses and organizations enhance their cybersecurity measures. NIST's Cybersecurity Framework (CSF) is a voluntary guide that helps organizations manage and reduce cybersecurity risks.

Our assessment of SBOT's controls was aimed at identifying the requirements necessary to achieve the organization's preferred level of maturity consistent across all cybersecurity risk management practices, including Identify, Protect, Detect, Respond, and Recover.

## Detailed Findings and Management Response

This section was removed from this public report due to the sensitive nature and risks associated with information technology security.