STATE BAR OF TEXAS
Internal Audit Services

AN INTERNAL AUDIT OF

Information Technology

Report No. 22-001

November 30, 2021

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 will impact these risks and internal controls in ways that this report cannot anticipate.

Table of Contents

Section Page Number

INTRODUCTION 5

OBJECTIVE 5

FINDING VS IMPROVEMENT OPPORTUNITY 6

CONCLUSION AND INTERNAL CONTROL RATING 6

McConnell Jones

December 6, 2021

Mr. David N. Calvillo
State Bar of Texas (SBOT) Audit & Finance Committee
1414 Colorado Street, 3rd Floor
Austin, TX 78701

Dear Mr. David N. Calvillo and Audit & Finance Committee Members:

Attached is Internal Audit Report #22-001 Information Technology Audit. This audit was performed as part of the approved Annual Internal Audit Plan.

Our review concluded that, overall, the State Bar of Texas' Information Technology Department has implemented management controls and processes to protect the agency's information and technology, however some improvement is needed.

Please contact Darlene Brown at 281.740.0017 if you should have any questions about this audit report.

Sincerely,

Darlene Brown

Darlene Brown, CIA, CFE, CSM

Partner

9130 Jollyville Road

Suite 320

Austin, TX 78759

Phone: 713.968.1600

WWW.MCCONNELLJONES.COM

Audit Report Highlights

Information Technology Audit

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 Annual Internal Audit Plan.

Audit Objectives and Scope

The purpose of this audit was to assess the State Bar of Texas' Information Technology (IT) management controls and processes in place to protect their information and technology.

Audit Focus

- Security policy administration. – Security policy components; security policy enforcement; employee IT security training.
- Security plan. – Security plan contents and updates.
- Data protection. – Processes, tools, and systems in place to protect confidential data.
- Incident response plan. – Incident response plan content; incident monitoring; incident reporting; corrective actions.
- Change management processes. – Change management policy; change management program; patch application processes; system development and testing processes.
- Information technology strategic planning. – IT strategic plan content, review, and updates.
- Compliance with applicable statutes and policies.

Audit Conclusion

Our review concluded that overall, a management control structure is in place to protect the agency's information and technology.

Internal Control Rating

Some Improvement Needed.

What Did We Recommend?

- Update IT security plan in the Information Technology Division Policies and Procedures Guide (IT Guide).
- Conduct annual risk assessment of IT environment.
- Update the IT Guide to incorporate all key policies.

The remaining recommendations are improvement opportunities for management to implement best practices.

Number of Findings/Opportunities by Risk Rating

Category	High	Medium	Low	Total
Findings	1	2	0	3
Improvement Opportunities	0	0	10	10

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

INTRODUCTION

McConnell & Jones LLP (MJ) performed an internal audit of the Information Technology Department's controls and processes.

We performed this audit as part of the approved FY 2021 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.

Pertinent information has not been omitted from this report. This report summarizes the audit objective and scope, our assessment based on our audit objectives and the audit approach.

Background

Information technology (IT) rated high on the risk assessment due to the impact on SBOT operations if the network or systems go down or if the systems are compromised. Additionally, a significant amount of confidential and sensitive data is maintained on these systems, including attorney license status. Furthermore, significant changes have occurred with the way information technology is used to support remote working and training during the pandemic.

OBJECTIVE

The purpose of this audit was to assess management controls and processes in place to protect the agency's information technology and data.

Our audit addressed the following questions related to risk, controls, processes, and reporting:

- Are SBOT's information technology policies comprehensive and enforced to protect the organization?
- Does SBOT's security plan address, and align with, key risk areas of SBOT's IT environment?
- Does SBOT's IT processes, tools and systems protect confidential and sensitive data?
- Are processes in place that would allow SBOT to quickly respond to an incident that compromised confidential and sensitive data?
- Are change management processes in place to ensure that new applications, system updates and patch applications do not negatively impact operations?
- Is an IT strategic plan in place to prioritize IT hardware and software needs?

As such the audit focused on the following processes:

- Security policy administration. – Security policy components; security policy enforcement; employee IT security training.
- Security plan. – Security plan contents and updates.
- Data protection. – Processes, tools, and systems in place to protect confidential data.
- Incident response plan. – Incident response plan content; incident monitoring; incident reporting; corrective actions.
- Change management processes. – Change management policy; change management program; patch application processes; system development and testing processes.
- Information technology strategic planning. – IT strategic plan content, review, and updates.

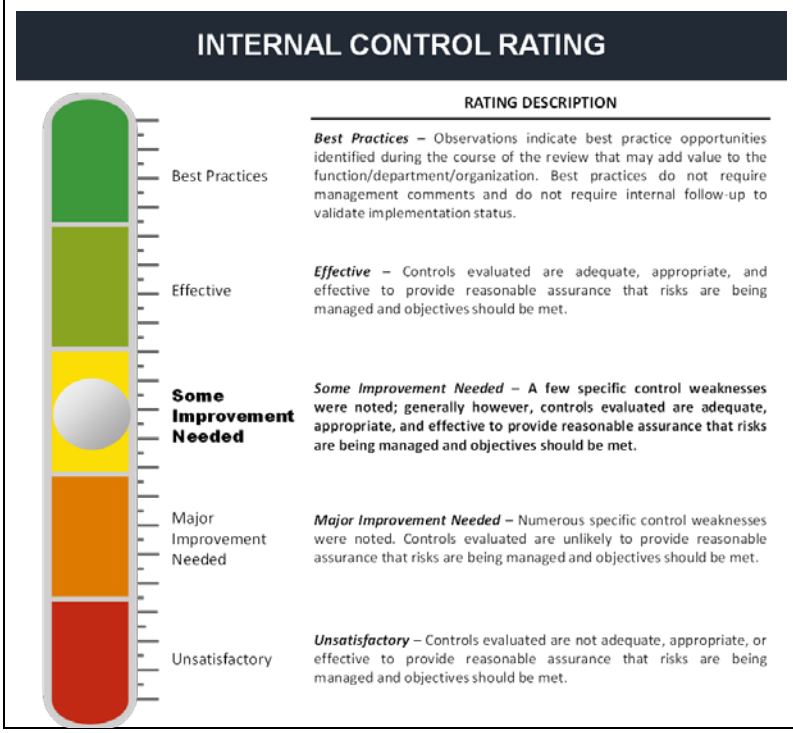
- Compliance with applicable statutes and policies.

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.

CONCLUSION AND INTERNAL CONTROL RATING

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



SBOT has established policies and procedures for information technology and data. However, a few specific control weaknesses were noted.

In general, controls evaluated are adequate, appropriate, and effective to provide reasonable assurance that the State Bar of Texas' Information Technology (IT) management controls and processes in place protect their information and technology.

Exhibit 1: Internal control rating description.