Texas Lottery Commission

Internal Audit Services

AN INTERNAL AUDIT OF:

Agency Cybersecurity Program

Report No. 19-008

January 17, 2020

FINAL

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.

MJ McConnell & Jones LLP
CERTIFIED PUBLIC ACCOUNTANTS

Audit Report Highlights
Agency Cybersecurity Program

Why Was This Review Conducted?

McConnell & Jones LLP (MJ) serving as the outsourced internal audit function (Internal Audit) for the Texas Lottery Commission (TLC) performed this internal audit as part of the approved FY 2019 Annual Internal Audit Plan.

Audit Objectives and Scope

The purpose of this review was to provide TLC leadership with assurance that their Information Technology (IT) security processes meet compliance requirements established by the state of Texas and addresses audit findings noted in recent external audits.

The audit period was for the agency's cybersecurity program and prior audit report findings remediation status as of July 2019.

Audit Focus

This review focused on the following areas:

1. Cybersecurity program governance.
2. Prior external security study findings' remediation status.
3. Prior MUSL review findings' remediation status.
4. Addressing penetration testing results.
5. Third-party cybersecurity audit focus.
6. Agency 2018 security plan submitted to the Department of Information Technology (DIR).
7. Processes and tools used to manage personal identifiable information (PII).
8. Agency incident response plan and processes.
9. Patch management.

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

Audit Conclusions

The agency has established an effective cybersecurity program that includes processes and activities that extend beyond the minimum requirements established by the state of Texas and the Department of Information Resources.

The United States Department of Homeland Security defines cybersecurity as the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

Protecting the agency against cybersecurity treats and data security is at the forefront of the agency's leadership team and the Information Technology Department. To this effect, the agency has developed a monitoring and oversight function that is effective in governing the agency's cybersecurity framework.

We also determined through our audit procedures that the agency has ensured the audits conducted by third-parties address key risk areas related to cybersecurity as well ensuring compliance with the state of Texas mandates outlined in Texas Administrative Code (TAC) 202.

Internal Control Rating

Best Practices

What Did We Recommend?

We had no reportable findings and therefore no recommendations are made for the agency's cybersecurity program.

Number of Findings by Risk Rating

High	Medium	Low	Total
0	0	0	0

INTRODUCTION

McConnell & Jones LLP (MJ) serving as the outsourced internal audit function (Internal Audit) for the Texas Lottery Commission (TLC) performed an internal audit of the agency's cybersecurity program.

We performed this audit as part of the approved FY 2019 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.

OBJECTIVE

The purpose of this review was to provide TLC leadership with assurance that their Information Technology (IT) security processes meet compliance requirements established by the state of Texas and addresses audit findings noted in recent external audits.

Specifically, we designed audit procedures to:

1. Determine if documentation and tools supporting the governance of the agency's cybersecurity program addresses key risk areas and that policies and procedures are updated.
2. Assess the current status of remediation efforts being completed to address audit findings noted in the agency's latest security study.
3. Assess the current status of the remediation efforts being completed to address audit findings noted in the agency's latest MUSL audit.
4. Ensure that the agency has process in place to assess penetration testing results and take appropriate actions.
5. Determine if third-party cybersecurity audits address key risk areas and the state of Texas compliance requirements.
6. Determine if the 2018 security plan submitted to the Texas Department of Information Resources (DIR) addresses and aligns to key risk areas within TLC's information technology environment.
7. Determine if the agency's processes, tools and systems used to manage personal identifiable information (PII) ensures data management risks are effectively addressed.
8. Determine if policies, procedures and supporting tools related to the incident response program ensure risk areas are effectively addressed.
9. Assess TLC's patch management program to ensure it reduces the agency's risk exposure by addressing key patches in an effective manner.

SCOPE

The audit period was for the agency's cybersecurity program and prior audit report findings' remediation status as of July 2019. This work product was at a point in time evaluation that cannot address the inherent dynamic nature of subsequent changes to the process and procedures reviewed.

PROCEDURES PERFORMED

We conducted interviews, business process walkthroughs, reviews of written policies and procedures, reviewed prior audit reports and conducted sample testing of supporting documentation.

CONCLUSION AND INTERNAL CONTROL RATING

*Our audit procedures applied resulted in an overall internal control rating of **Best Practices**. **Figure 1** describes the internal control rating.*

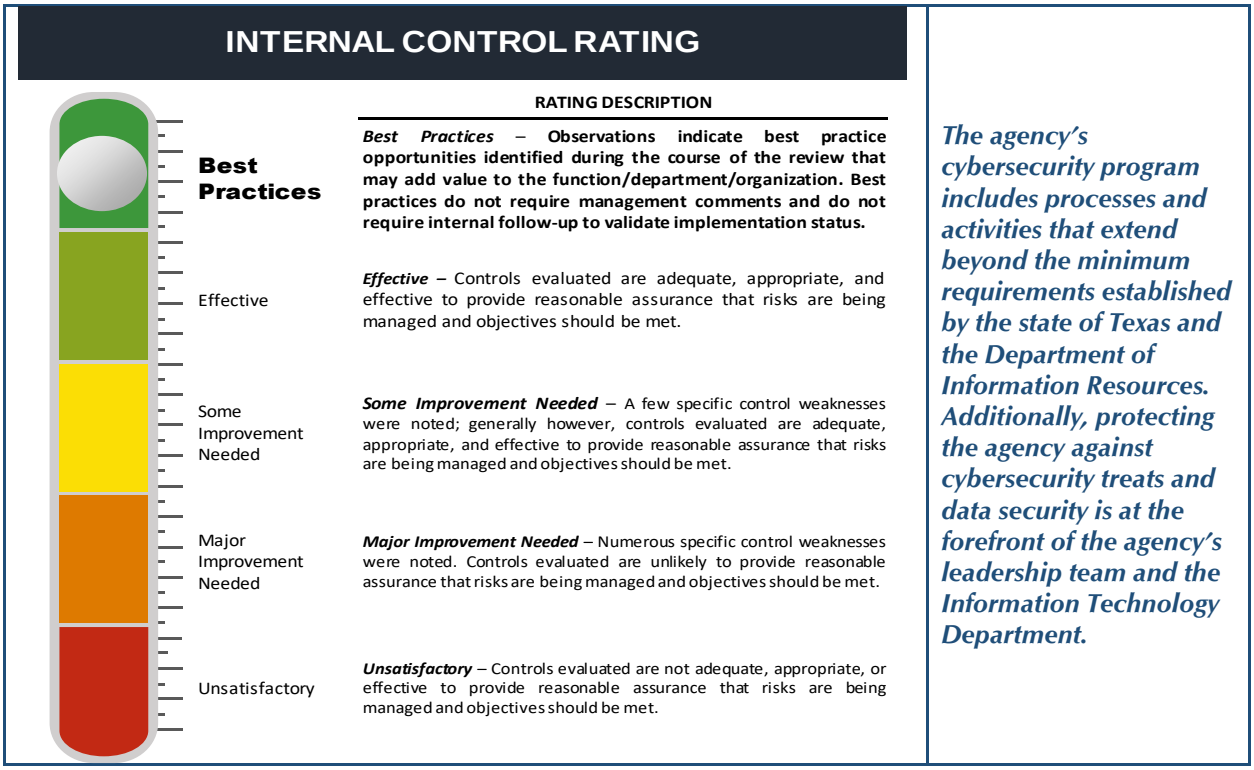

Figure 1 Internal control rating description.

TLC CYBERSECURITY PROGRAM OVERVIEW

This section of the report provides a summary overview of TLC's cybersecurity program controls. .

This report does not discuss the agency's specific cybersecurity program procedures, tools and processes as a such discussion could unnecessarily expose the agency to potential threats.

Compliance with State Information Technology Regulations

TLC has effective policies, processes and tools in place to ensure compliance with all applicable information technology regulations. Texas legislators recognized the importance of information technology security and enacted statutes to establish minimum requirements that stat agencies must follow. These include:

- Government Code 2054 Information Resources (Information Resources Management Act)
- HB 8 The Texas Cybersecurity Act

Government Code 2054 designates the Department of Information Resources to coordinate and direct the use of information resources technologies by state agencies. Section 2054.007 exempts the Texas Lottery Commission from the Act's planning and procurement requirements. Section 2054 (b) requires DIR to develop and publish policies, procedures, and standards relating to information resources management by state agencies. As such, DIR established rules in the Texas Administrative Code (TAC) Chapter 202.

TAC 202.24 requires each agency to develop a documented information security program. TAC 202.24 also defines what should be included in each agency's information security program.

TLC's cybersecurity program and processes ensure compliance with the state of Texas requirements established by DIR through TAC 202 Information Security Standards. **Figure 2** compares the guidance provided by DIR and TAC 202 requirements to TLC's cybersecurity program.

TAC 202 Requirements and DIR Guidance	TLC's Cybersecurity Program
Agency maintains agency-wide information security plan.	✓
Agency has developed policy and procedures with continuous review and development.	✓
Agency works with third-party vendors to ensure business and technical resources are available to maintain the agency's cybersecurity environment.	✓
Developed training programs are in place to ensure cybersecurity awareness and knowledge is made available to the entire agency.	✓
Developed monitoring and oversight functions are in place to ensure cybersecurity threats are addressed effectively.	✓
The agency maintains an environment that measures the risks related to protection of the agency's IT assets which includes hardware, software and data.	✓
The agency has matured processes and well-experienced staff maintaining the agency's cybersecurity functions.	✓
The agency maintains an inventory of items requiring oversight and monitoring to ensure the protection of IT assets.	✓
The agency ensures that the executive level, commissioners and governing agencies are aware of the agency's cybersecurity programs and identified areas of opportunity.	✓

Figure 2 DIR and TAC 202 Requirements Compared to TLC's Cybersecurity Program

Legend: ✓ = TLC Meets this Requirement

Compliance with State Information Technology Security Requirements

TLC ensures compliance with state information security requirements through various processes and activities. One of these activities is to request external audits and reviews. Audit procedures applied during the agency's requested external audits and reviews of the agency's information technology security assess DIR's 24 control standards and ensures compliance with applicable state requirements. These third-party external audits also provide assurance that TLC's cybersecurity framework is tested by an independent entity and provides specialized recommendations on areas that require attention.

We compared the TAC 202 requirements to audit objectives and focus of each of the three external audits regularly requested by the agency. **Figure 3** documents the 24 control standards and which of the three regularly requested external audit address the respective key attribute. The graph also documents TLC's success in using third-party audits to address internal risk areas as well as state compliance initiatives.

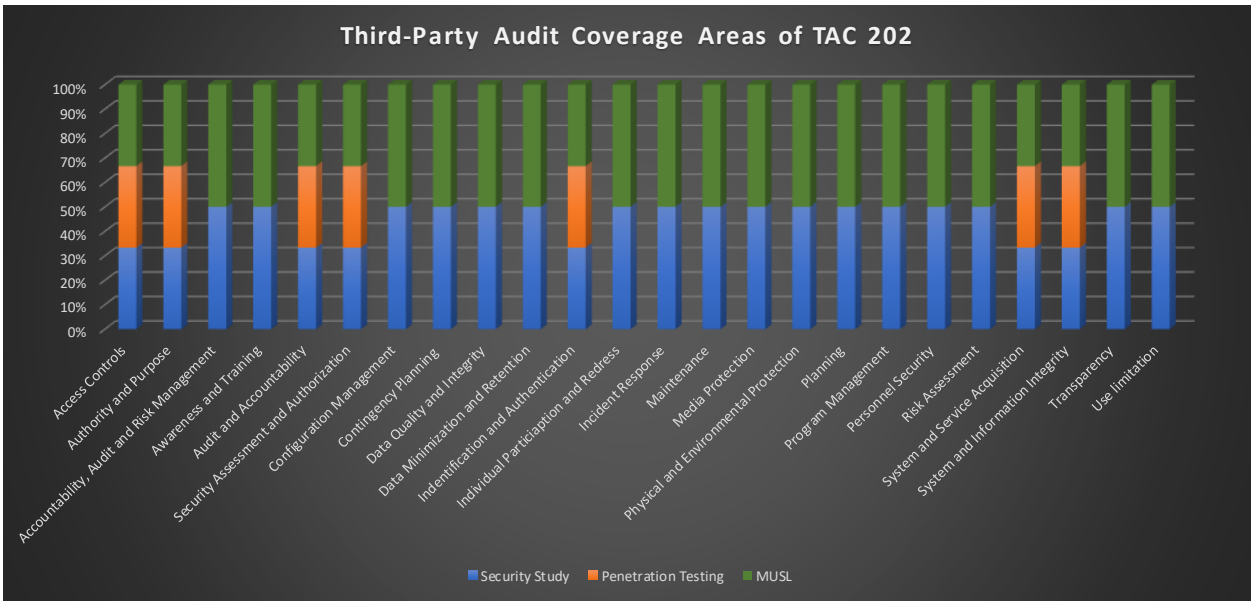

Figure 3 Third-Party Audit Coverage Areas of TAC 202 Requirements

Agency Security Plan

TLC is compliant with Government Code Sec. 2054.133 which requires state agencies in Texas to develop and periodically update an information security plan. The security plan submitted to DIR by TLC's Information Security Officer (ISO) is compliant with TAC 202 and the agency's policy and procedures. Our assessment of the ratings entered on the security plan by the agency were reasonable with supporting documentation illustrating the agency's control activities.

We noted that the security plan document discusses key areas and the current status of TLC's cybersecurity efforts. The documentation provided by TLC and verified through our interviews provide assurance that TLC's staff understand the agency's cybersecurity framework and areas that require development. This also supports our conclusion that the agency understands its risk environment and is effectively managing it with current resources. The security plan document also accounts for the overall maturity of the procedures completed by the agency.

We also noted that the information entered into the security plan by the ISO is reflective of the agency's current efforts to address the audit findings noted by the bi-annual security study report that was issued in FY 2019 and the penetration testing conducted by a third-party during this audit scope period.

Personal Identifiable Information Protection

The agency's personal identifiable information program is an on-going process that ensures key data assets are managed with effective PII protocols. We noted that the agency has developed a ticket system that is used by the agency to track the progress of an IT project. This system notes key documentation areas and procedures that have been completed to date and details on the on-going process in-progress. The agency also provided us with documentation listing the data types that are considered PII. Our review of the data types certified as PII is reasonable based on the information handled by agency staff.

The agency has also documented policy, procedures and training to provide assurance that agency staff understand how personal identification information should be handled.

Incident Response Program

The agency has a well-documented and executed incident response program. We noted the agency's incident policy and procedures are maintained and updated by staff based on the agency's policy update program. These policies and procedures are located on the agency's intranet which provides accessibility by authorized agency staff.

TLC defines an information technology event as any observable occurrence in a system or network. A cybersecurity incident is defined as a violation or imminent threat of violation to the security (availability, integrity or confidentiality) of agency information resources by an adverse event. Our review of the applicable policy and procedures indicates that the documentation represents the attributes of a defined purpose, responsibility, documented processes, and effective policy management.

We also noted through testing of a sample of incident reports that the agency has processes in place to detect potential incidents, followed their policy and procedures, and maintained state compliance by advising DIR of the respective incident and completing the required monthly incident reports.

Information Technology Patch Management Program

The agency has developed a systematic framework for patch management. Within the information technology environment, a patch is a set of changes to a computer program or data that is designed to fix, update or improve the program or data. Most often, patches are issued to correct potential security vulnerabilities. It is crucial to any organization to have a documented, thoughtful process to evaluate and test patches before they are applied to minimize unintended consequences.

TLC has developed policy and procedures defining the key areas and responsibilities of the patch management process. This ensures that staff have an understanding of the process. Our assessment of the patch management process determined the agency has an effective patch management program, documents the servers receiving patches and upgrades with assigned persons and the purpose or function of the server. We also noted that the agency documents the date of each update. This documentation helps to ensure applied patches are performed within a systematic framework.

External Audit Findings Remediation

TLC has processes in place to ensure that audit and penetration testing findings are addressed in a timely manner. TLC receives a multitude of external and internal audits, some of which focus specifically on information technology security and others include components of information technology. As previously discussed, the agency also requests certain external audits be performed to ensure they are compliant with statutes and administrative codes while also providing insight into areas where they can improve their information technology security to provide assurance key agency assets are protected.

One of the requested external audits is the bi-annual security study required by Texas statute and another is regular penetration testing. These audits and penetration testing are directly related to cybersecurity initiatives. Another requested external review is performed by MUSL and is specific to agency lottery operations, but also includes testing and oversight of areas related to cybersecurity. These types of audits provide the agency a value-added approach to address key cybersecurity areas and ensures consistent oversight and monitoring of the cybersecurity function.

The agency takes audit findings seriously and has processes in place to ensure accountability for implementing corrective actions in a timely manner. The agency developed an internal database program to maintain audit findings, assign remediation responsibility within the agency and track status. This provides assurance that audit findings receive developed action plans with specific assignment responsibilities and follow-up.

We reviewed the following reports to determine the nature of any audit findings, recommendations and management responses:

- 2018 security study performed by a third-party vendor
- 2018 MUSL compliance review
- Penetration testing results

We were able to determine that remediation actions taken were reasonable to address the respective audit finding. We were also in agreement with the current status of the audit finding which were either completed or in the process of being completed.

Our review of the documentation provided, and interviews conducted determined that the agency has developed a systematic framework to communicate, follow-up, provide oversight, monitoring, responsibility and action to close audit findings. The following areas were reviewed and determined to be effective:

Communication –Audit findings are effectively communicated to and addressed by assigned agency staff.

Documentation – The agency effectively documents the audit findings in a central database that documents the finding, severity ranking, action status, and responsible person.

Assurance – The agency documents the assigned person responsible for addressing the audit finding with documentation if the action item has been completed. If the item is pending the agency maintains documentation until the action item has been closed.

Figure 4 provides a comparison summary of the agency's audit finding governance activities to our audit testing results. Our audit testing noted that TLC effectively managed 100 percent of the audit findings we reviewed.

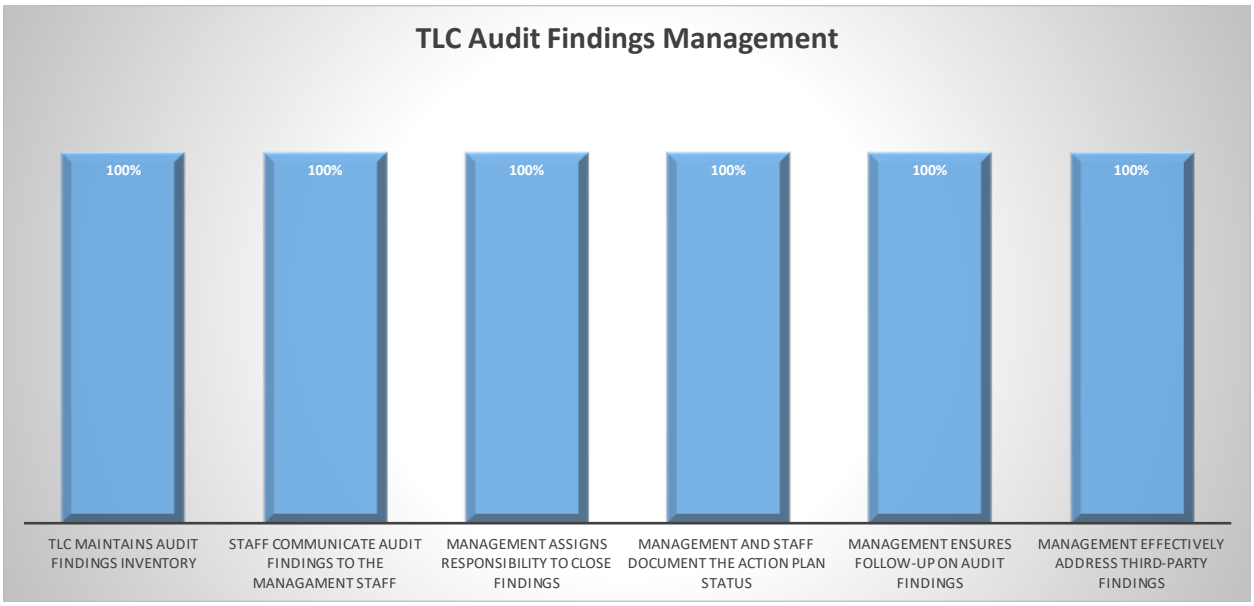

Figure 4 TLC's Management of Audit Findings