TEXAS LOTTERY COMMISION

Internal Audit Services

AN INTERNAL AUDIT OF

Confidential Data

Report No. 22-001

August 29, 2022

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.

Report Highlights

Why Was This Review Conducted?

McConnell & Jones LLP (MJ) serving as the outsourced internal audit function (Internal Audit) for performed this internal audit as part of the approved FY 2022 Annual Internal Audit Plan.

Audit Objectives and Scope

The purpose if this audit was to review Texas Lottery Commission's (TLC) business processes and internal controls related safeguard confidential data and anonymity of prize winners when requested.

The audit scope period was FY2021 and FY2022 YTD.

Audit Focus

1. To evaluate controls in place to ensure physical and electronic confidential data is properly secured including:
   - Identification
   - Classification
   - Handling and Storage (destruction)

2. Follow-up on the FY2018 Personally Identifiable Information (PII)audit report recommendations.

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

TLC has implemented numerous controls to provide reasonable assurance of the protection of confidential data, especially anonymous claims information. Additionally, the Agency has implemented access controls, physical and logical, we consider to be best practice processes.

We did identify three opportunities to enhance current policies and processes. One is to enhance existing policies regarding disclosure of anonymous claims.

Our follow-up on the FY2018 PII Audit Report, found TLC has implemented all the opportunity for improvement recommendations. No recommendations were made for control deficiencies.

Internal Control Rating

Best Practices for Access Controls and Generally Effective Overall.

What Did We Recommend?

1. We made no recommendations related to internal controls.

Number of Findings/ Opportunities by Risk Rating

Category	High	Medium	Low	Total
Findings	0	0	0	0
Improvement Opportunities	0	0	3	3

Introduction

McConnell & Jones LLP (MJ) performed an internal audit of Confidential Data.

We performed this audit as part of the approved FY 2022 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, Conclusion, and Internal Control Rating

This audit identified findings that resulted in an overall internal control rating of ***Best Practices for Access Controls*** *and* ***Generally Effective overall****.* ***Exhibit 1*** *describes the internal control rating.*

The purpose of this audit was to assess Texas Lottery Commission's (TLC) data classification and handling processes to determine effectiveness and possible improvement opportunities to ensure data is secure and prize winners remain anonymous if they elect that option.

As such we focused on the controls which ensure physical and electronic confidential data is properly secured including:

1. Identification
2. Classification
3. Handling and Storage (destruction)
4. Follow-up on PII audit report recommendations.

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.

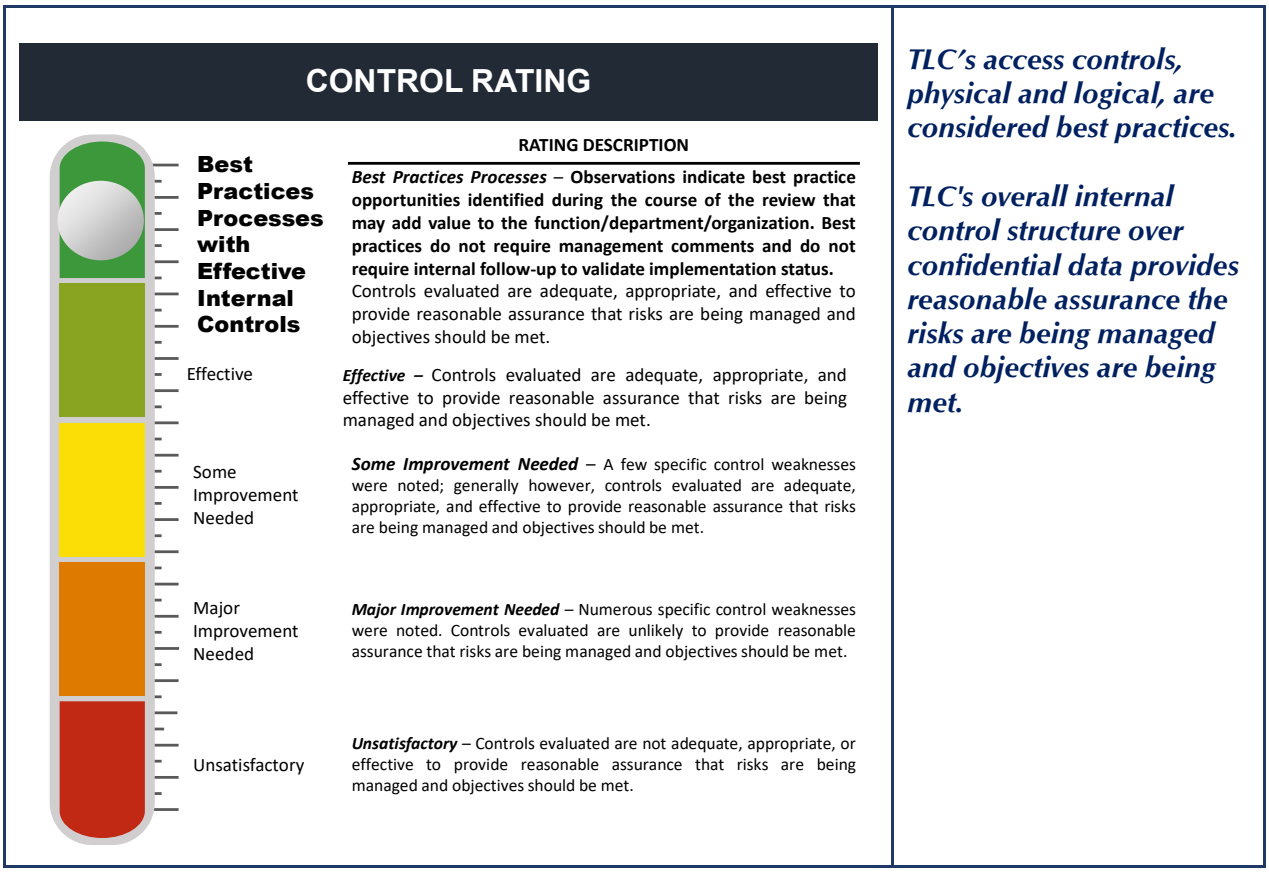

Exhibit 1: Internal control rating description.

Observation and Risk Rating Summary

Exhibit 2 *provides a summary of our audit observations. See the business risk section of this report for a discussion of all issues identified, recommendations, and management responses.*

Business Objective	Internal Control Rating	Control Assessment / Findings	Recommendations
1. TLC data classification and handling processes ensure data is secure and prize winners remain anonymous when they elect that option.	Generally Effective	No findings noted. *Opportunity for Improvement:* Processes to be followed in the event of a disclosure of anonymous claims have not been formally documented.	No recommendations are made. Update the current policies and procedures to include the actions necessary in the event of disclosure or anonymous claims. Additionally, TLC should test the procedure by simulating an actual event, to

Business Objective	Internal Control Rating	Control Assessment / Findings	Recommendations
			determine if the procedure has any gaps.
1. TLC physical and logical access controls ensure confidentiality of claims data.	Best Practice Processes	No findings noted. *Opportunity for Improvement:* Within the Claims Center, it is possible for personnel to view the screens of other users.	No recommendations are made. Consider using screen protectors or a filtering solution to prevent individuals from viewing information on the screen of Claims Center personnel.
2. TLC data retention and destruction processes ensure data is maintained only as long as necessary and is destroyed in a secure fashion when no longer needed.	Generally Effective	No findings noted. *Opportunity for Improvement:* The TLC retention schedule does not address the retention of Jackpot claims stored within the warehouse.	No recommendations are made. Include Jackpot claims retention parameters for the Jackpot claims stored within the warehouse prior to the next recertification of the Records Retention Schedule in prior to submission to the Texas State Library and Archives Commission in October 2026.

Detailed Findings and Management Response

This section of our report provides a discussion on the reportable findings we noted during the audit, our recommendations, and managements response.

Business Objective #1: TLC data classification and handling processes ensure data is secure and anonymous claimants remain anonymous.

Risk Ranking: **Generally Effective**

Observations

- The TLC Information Resources Security Manual (IRSM) details the data classification levels which establish the appropriate protective measures (technical and non-technical) needed to minimize the risk of unauthorized modification, deletion, or release of the information.
- Requests through the Public Information Act flow through the Public Information Coordinator, to ensure confidentiality of information released.

- Requests for anonymity are documented on the claim form and updated within the IGT ES system.

Opportunity for Improvement:

1. TLC current policies and procedures do not include the detailed steps to take in the event of disclosure of anonymous claims.

Recommendations #1

No recommendations are made.

Opportunity for Improvement Recommendation:

1. Update the current policies and procedures to include the actions necessary in the event of disclosure or anonymous claims. Additionally, TLC should test the procedure by simulating an actual event, to determine if the procedure has any gaps.

Managements Response #1

Management response is not required for improvement opportunities not related to internal controls or process efficiencies.

Business Objective #2: TLC physical and logical access controls ensure confidentiality of claims data.

Risk Ranking: **Best Practice Processes**

Observations

- All employees receive Texas Department of Information Resources approved training as well as PII training.
- Data classification policies are documented in the Information Resource Security Manual.
- Access reviews of key systems performed.
- Changes to claims are logged within system.
- Security conduct routine walkthrough to verify doors remained locked at appropriate times, access system is functioning properly, and cameras are recording.
- Physical controls implemented at Claims Center and Warehouse to protect data.
- Electronic security badge access in place.
- Documented policies and procedures covering:
    - Physical security,
    - Cyber security detection and response,
    - Rules for granting, managing, monitoring and removal of physical access to information resources facilities.
    - Employee access to confidential information and appropriate usage.

Opportunity for Improvement:

1. Within the Claims Center, it is possible for personnel to see the screens of other users, as a screen protector/filtering is not in place.

Recommendations #2

No recommendations are made.

Opportunity for Improvement Recommendation:

1. Consider using screen protectors or a filtering solution to prevent individuals from viewing information on the screens of Claims Center personnel.

Managements Response #2

Management response is not required for improvement opportunities not related to internal controls or process efficiencies.

Business Objective #3: TLC data retention and destruction processes ensure data is maintained only as long as necessary and is destroyed in a secure fashion when no longer needed.

Risk Ranking: **Generally Effective**

Observations

- Physical storage of claims data is maintained at the TLC claims center and warehouse, as well as the Texas State Library and Archives Commission (TSLAC).
- Physical access to the claims center and Warehouse is restricted.
- Claims that have met their retention date are reviewed by Records Retention Coordinator, with destruction through a third-party vendor.
- Policies and procedures address records retention digital media sanitation.

Opportunity for Improvement:

1. The TLC retention schedule does not address the retention of Jackpot claims stored within the warehouse.

Recommendations #3

No recommendations are made.

Opportunity for Improvement Recommendation:

1. Include the retention parameters for the Jackpot claims stored within the warehouse prior to the next recertification of the Records Retention Schedule in prior to submission to the Texas State Library and Archives Commission in October 2026.

Managements Response #3

Management response is not required for improvement opportunities not related to internal controls or process efficiencies.

Business Objective #4: TLC has addressed processes improvements identified to ensure the continued effectiveness of the TLC's processes and controls over PII handling.

Risk Ranking: **Generally Effective**

Observations

Our follow-up on the FY2018 PII Internal Audit Report, found TLC has implemented all the opportunity for improvement recommendations. No recommendations were made for control deficiencies. We noted that:

1. A Comprehensive Data Security and Privacy Program Coordination is in place.
2. Information inventory and mapping is in place.
3. All TLC employees receive training approved by Texas Department of Information Resources which includes information about sensitive and confidential data.

Recommendations #4

No recommendations are made.

Managements Response #4

None required.

APPENDIX A - BACKGROUND

This section of the report provides an overview of the Texas Lottery Commission's controls to secure confidential data, including ensuring anonymous claimants remain anonymous.

Protecting confidential data is engrained in the Texas Lottery Commission's (TLC) staff, processes, procedures, and systems. Confidential data comes in many forms at TLC including personally identifiable information of claims winners, requested anonymity of million dollar or more claims winners.

To assure appropriate data remains confidential, TLC has implemented a data classification policy and process for identifying data as either public, sensitive, and confidential. They have implemented numerous policies and procedures to assure confidential data is secure.

In additional to maintaining a secure environment, physical and logical, for confidential data, they have also implemented policies and procedures for the destruction of confidential data in a secured manner. TLC maintains claims data for five (5) years, with the exception being jackpot winners and claims retained for legal proceedings.

APPENDIX B - BUSINESS OBJECTIVES, RISKS, FINDINGS AND MANAGEMENT RESPONSE

This section of the report provides a summary of the function's key business objectives, primary business risks, management's controls in place and the respective internal control assessment. Each table also includes our recommendations to address deficiencies noted, or opportunities to enhance current controls.

1 BUSINESS OBJECTIVE: ***DATA CLASSIFICATION***	
Business Objective	To implement and maintain data classification and handling processes that ensure data is secure and prize winners remain anonymous when they select that option.
Business Risk	▪ Data classification policies and procedures may not be in place to ensure data is properly identified, classified, and labels to ensure appropriate handling and storage.
Management Controls in Place	▪ Requests for anonymity are documented on the claim form and updated within the IGT ES system. ▪ In the event of a disclosure of anonymous winner, TLC would reach out to the requestor and notify the claimant. ▪ Requests through the Public Information Act flow through the Public Information Coordinator, to ensure confidentiality of information released. ▪ The TLC Information Resources Security Manual (IRSM) details the data classification levels which establish the appropriate protective measures (technical and non-technical) needed to minimize the risk of unauthorized modification, deletion, or release of the information. ▪ The boxes of claims stored in the warehouse for storage are labeled with the record series title, year(s) of record(s), retention period, destroy date, and the division box number.
Control Tests	▪ Interviewed key process owners. ▪ Reviewed the TLC Information Resources Security Manual ▪ Conducted walkthrough of the TLC Warehouse and Claims Center ▪ Sample tested claims to determine access within IGT ES application
Control Assessment / Findings	Generally Effective ▪ Controls are working effectively. No control findings noted. <u>*Opportunity for Improvement*</u> 1. Processes to be followed in the event of a disclosure of anonymous claims have not been included in the current policies and procedures.
Recommended Actions	<u>*Opportunity for Improvement*</u> Update current policies and procedures to include the actions necessary in the event of disclosure or anonymous claims. Additionally, TLC should test the procedure by simulating an actual event, to determine if the procedure has any gaps.

2 BUSINESS OBJECTIVE: *ACCESS CONTROLS*	
Business Objective	To implement and maintain physical and logical access controls that ensure confidentiality of claims data.
Business Risk	▪ Unauthorized access or disclosure of PII collected on claims forms may occur. o Prize winners may ay not remain anonymous when they elect that option. o Physical controls for document storage may not be secure and safe. o Chain of custody may not be maintained. o Logical access controls may not secure digital documentation.
Management Controls in Place	▪ Data classification policies and procedures are documented in the Information Resources Security Manual (IRSM). ▪ TLC has implemented PII Training (Annual and on New Hire). ▪ IT systems are classified three tiers of data (Confidential, Sensitive, and Public). ▪ Access reviews of the IGT ES system are performed annually. ▪ Changes to claims within IGT ES are logged. ▪ TLC has implemented physical controls in the Claims Center and Warehouse to protect claims data. ▪ Security contractors routinely conduct security walkthroughs to make sure that doors remain locked after hours, that the access system is functioning properly, that cameras are recording properly. ▪ The IGT ES Dashboard System Admin section is used to manage the users, groups, and roles. ▪ Review of IGT ES access is conducted annually. ▪ TLC leverages a master tracking tool which details the box containing individual claims by date range. ▪ Claims stored in the mezzanine of the warehouse, are housed in multi-tiered cages which are key-locked. Additionally, the keys are stored in a master key lock box when not in use. ▪ The TLC Information Resources Security Manual (IRSM): o Establishes the rules for granting, managing, monitoring and removal of physical access to information resources facilities. o Identifies the individuals or groups within the agency and their responsibilities as they relate to agency information, including the authority to permit users or groups of users to have access to that information. ▪ Policies and procedures regarding handing security incidents, cybersecurity, and employee access to confidential information are in place.
Control Tests	▪ Interviewed key process owners. ▪ Walkthrough of the TLC Warehouse and Claims Center ▪ Tested Key and Security badge access to the Claims Center & Warehouse ▪ Sample tested claims to determine access within IGT ES application ▪ Reviewed the following data access policies and procedures: o TLC Information Resources Security Manual o Information Security Incident Reporting

2 BUSINESS OBJECTIVE: *ACCESS CONTROLS*	
	○ Cybersecurity Incident Detection and Response ○ Information Security Training ○ Personnel Handbook
Control Assessment / Findings	Best Practice Processes ▪ Controls are working effectively. No control findings noted. <u>*Opportunity for Improvement*</u> 1. Within the Claims Center, it is possible for personnel to see the screens of other users, as a screen protector/filtering is not in place
Recommended Actions	<u>*Opportunity for Improvement*</u> Implement a screen protector/filtering solution to prevent individuals from seeing information on the screen of Claims Center personnel.

3 BUSINESS OBJECTIVE: *RETENTION & DESCTRUCTION*	
Business Objective	To implement and maintain data retention and destruction processes that ensure data is maintained only as long as necessary and is destroyed in a secure fashion when no longer needed.
Business Risk	▪ Handling, storage, and destruction of claims may not comply with records retention requirements (digital and hard copy).
Management Controls in Place	▪ Physical storage of claims data is maintained at the TLC claims center and warehouse, and the Texas State Library and Archives Commission (TSLAC). ▪ Physical access to the claims center and Warehouse is restricted. ▪ Claims that have met their retention date are submitted to and reviewed by the Records Retention Coordinator, with destruction occurring through a third party. ▪ TLC leverages a master tracking tool which details the box containing individual claims by date range. ○ The boxes of claims in the storage warehouse are labeled with the record series title, year(s) of record(s), retention period, destroy date, and the division box number. ▪ The TLC 2021 Records Retention Schedule details the recertification of the TLC Records Retention Schedule with the Texas State Library and Archives Commission. The schedule details the specific retention period for TLC data/documentation based on how the data (record type) is classified. ▪ The Records Retention Procedure details the guidelines to ensure TLC records are retained and disposed in accordance with the agency's records retention schedule and state rules. ▪ TLC has a developed a Request to Dispose of Documents email template, which the Records Retention Coordinator prepares when requesting disposal of records.

3 BUSINESS OBJECTIVE: ***RETENTION & DESCTRUCTION***	
	▪ The TLC Digital Media Sanitization details the procedure to ensure data storage devices containing sensitive or confidential information are sanitized in compliance with state and federal law.
Control Tests	▪ Interviewed key process owners. ▪ Conducted walkthrough of the TLC Warehouse and Claims Center ▪ Reviewed Tracking Tool (Printed) ▪ Reviewed the following data retention and destruction policies and procedures: o Records Retention Schedule o Records Retention Procedure o Request to Dispose of Documents request template o Digital Media Sanitization
Control Assessment / Findings	Generally Effective ▪ Controls are working effectively. No control findings noted. *Opportunity for Improvement* 1. The TLC retention schedule does not address the retention of Jackpot claims stored within the warehouse.
Recommended Actions	*Opportunity for Improvement* Include the retention parameters for the Jackpot claims stored within the warehouse prior to the next recertification of the Records Retention Schedule in prior to submission to the Texas State Library and Archives Commission in October 2026.

4 BUSINESS OBJECTIVE: ***Follow-up on PII audit report recommendations***	
Business Objective	To mitigate control issues identified during the FY2018 personally identifiable information (PII) audit.
Business Risk	▪ Control weaknesses identified during audit may not have been addressed.
Management Controls in Place	▪ The TLC Information Resources Security Manual, adopted April 19, 2022, details the data security and privacy program. ▪ Comprehensive Data Security and Privacy Program Coordination is in place. Specifically. o The Information Resources Security Manual defines the data security and privacy program. o TLC Privacy Statements on the Website (including the Bingo Website), Mobile App program, and Retailer's Manual reinforces the privacy program. o The Enterprise Risk Manager reviews the privacy program periodically and manages the Open Records program as per the Texas Public Information Act. ▪ Information Inventory and Mapping is in place. Specifically:

4 BUSINESS OBJECTIVE: ***Follow-up on PII audit report recommendations***	
	○ The Information Security Officer worked with the DBAs to inventory the TLC applications which contain PII. ○ The classification of PII was based on NIST definitions. ○ TLC can report on the status of PII data within the various applications. ○ The Information Data Officer is working to ensure all the applications are flagged as having PII, as applicable. ▪ All TLC employees receive training approved by Texas DIR which includes information about sensitive and confidential data.
Control Tests	▪ Interviewed key process owners. ▪ Reviewed the following policies and procedures: ○ 18-002 Personal Identifiable Information Audit Report ○ TLC Information Resources Security Manual
Control Assessment / Findings	Generally Effective ▪ TLC has implemented all opportunity for improvement recommendations. No recommendations were made for control deficiencies in the audit.
Recommended Actions	No recommendation are made for this as prior recommendations have been fully implemented.