Texas Lottery Commission

Internal Audit Services

AN INTERNAL AUDIT OF:

TLC Vendor Software Changes

Report No. 20-007

December 14, 2020

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
TLC Vendor Software Changes

Why Was This Review Conducted?
This audit was performed as part of the approved FY 2020 Annual Internal Audit Plan.

Audit Objectives and Scope
We performed this audit to assess management's internal control structure in place to ensure complementary controls are in place to assure changes to International Game Technology's (IGT) software are monitored, authorized, and tested by the Texas Lottery Commission (TLC). The scope period was FY 2020.

Audit Focus
This audit focused on the following areas:

- ✓ Complementary controls for software changes listed on IGT's System and Organization Controls (SOC) Report FY2020.
- ✓ IGT Database changes.

Roles and Responsibilities
The agency's Information Resources (IR) division is responsible for implementing and monitoring software change controls. The agency's Information Resources Director oversees IR staff and activities.

Audit Conclusions
TLC's management control structure over the complementary controls for IGT software changes provides adequate, appropriate, and effective controls to provide reasonable assurance that risks related to changes made to International Game Technology's (IGT) software are being managed and objectives should be met. Some improvement opportunities were noted.

Changes to IGT database require pre-authorization by TLC. However, we noted it is plausible that changes could be made without such authorization. TLC is dependent on IGT's internal controls to manage this control.

Internal Control Rating
Generally Effective.

What Did We recommend?
We provide the following three recommendations to enhance existing internal controls:

1. TLC should retain the results and approvals associated with Customer Acceptance Testing (CAT) testing activity with all artifacts\documents associated with the individual change for the agency's required three (3) year retention period. These should be retained in a centralized location, such as the agency's document repository system. *(Business Objective #4)*
2. TLC should formally document and retain evidence of approval associated with the refreshing of the CAT environment by IGT, work with IGT to formally document the Emergency Bug Fix process, and maintain a log of all EBFs, including the reason associated with the EBF. The agency should also update the Testing of Program Modifications AD-IR-SO-024 procedure to include specific requirements associated with post implementation testing by the business owner. *(Business Objective #5)*
3. We recommend amending the IGT contract to allow for an audit of the vendor's controls over database changes to validate that they are working or to specify that future SOC audits address the controls over database changes. *(Business Objective #7)*

The remaining recommendations are improvement opportunities for management to consider. They are primarily to formalize/ document processes in place and increase retention time for artifacts\documents used for monitoring, authorizing, and testing IGT software changes to three (3) years as required by TLC's approved record retention schedule.

Number of Findings/Opportunities by Risk Rating

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

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 process to monitor, authorize, and test changes to International Game Technology's (ITG) software prior to putting in production. The scope period was FY 2020.

We performed this audit as part of the approved FY 2020 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 meets 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.

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

OBJECTIVE

The purpose of this audit was to assess management's internal control structure in place to ensure that changes to International Game Technology's software is monitored, authorized, and tested by TLC.

We designed audit procedures to evaluate internal controls and processes over:

- ✓ Complementary Controls for Software Changes listed on IGT's System and Organization Controls (SOC) Report FY2020.
- ✓ IGT Database changes.

SCOPE

This audit period was FY 2020. The audit focused on Complementary Controls for Software Changes listed on IGT's SOC Report FY2020 and IGT database changes.

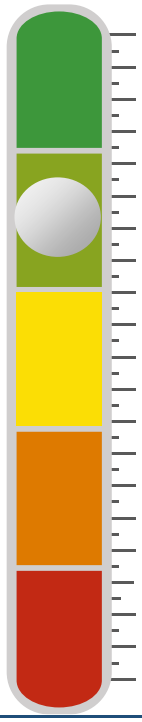
PROCEDURES PERFORMED

We conducted interviews and tested the complementary controls in place for IGT software changes and IGT database changes.

CONCLUSION AND INTERNAL CONTROL RATING

We concluded that overall internal controls are Generally Effective. ***Exhibit 1*** *describes the internal control rating.*

INTERNAL CONTROL RATING



	RATING DESCRIPTION
Best Practices	***Best Practices*** – Observations indicate best practice opportunities identified during the course of the review that may add value to the function/department/organization. Best practices do not require management comments and do not require internal follow-up to validate implementation status.
Generally Effective	***Generally Effective*** – **Controls evaluated are adequate, appropriate, and effective to provide reasonable assurance that risks are being managed and objectives should be met.**
Some Improvement Needed	***Some Improvement Needed*** – A few specific control weaknesses were noted; generally however, controls evaluated are adequate, appropriate, and effective to provide reasonable assurance that risks are being managed and objectives should be met.
Major Improvement Needed	***Major Improvement Needed*** – Numerous specific control weaknesses were noted. Controls evaluated are unlikely to provide reasonable assurance that risks are being managed and objectives should be met.
Unsatisfactory	***Unsatisfactory*** – Controls evaluated are not adequate, appropriate, or effective to provide reasonable assurance that risks are being managed and objectives should be met.

TLC's control structure provides adequate, appropriate, and effective controls to provide reasonable assurance that risks related to changes made to International Game Technology's (IGT) software are being managed and objectives should be met.

Exhibit 1: Internal control rating description.

OBSERVATION AND RISK RATING SUMMARY

Exhibit 2 *provides a summary of our improvement opportunities noted. See the business objective section of this report for a discussion of all issues identified, recommendations, and management responses.*

Number	Observation	Risk Rating
1	**CAT Approvals and Document Retention – Low Risk** TLC has processes in place for IGT system modification requests. However, we noted the following. *(Business Objective #4)* • There is no formal approval process of Customer Acceptance Testing (CAT) completion by the associated departments\Business Owners. • Weekly meetings with TLC Business Owners (major release) may have an agenda is in place, but no minutes are maintained.	

Number	Observation	Risk Rating
	• Multiple artifacts associated with an individual change are not maintained in a centralized location. ***Recommendation:*** TLC should retain the results and approvals associated with CAT testing activity, with all artifacts\documents associated with the individual change, in a centralized location.	
4	**CAT Processes – Low Risk** TLC's CAT procedures and approval of CAT system changes are not formalized. *(Business Objective #5)* • IGT is not required to obtain approval to refresh TLC's CAT environment. However, they do coordinate with TLC when a refresh is necessary. • An Emergency Bug Fix (EBF) testing process is not formally documented. • There is not a formal process ensuring Business Owners perform post implementation testing. ***Recommendations:*** 1. TLC should formally document and retain evidence of approvals associated with the refreshing of the CAT environment by IGT. 2. TLC should work with IGT to formally document the EBF process as well as maintain a log of all EBFs, including the reason for the fix. 3. TLC should update procedures to include specific requirement associated with post implementation testing by business owners.	
5	**IGT Database Administrator Activity – Low Risk** TLC does not have oversight into all activity performed by IGT Database Administrators (DBA) and must rely on IGT internal controls for monitoring and logging of all DBA activity, to ensure changes by DBAs are authorized. *(Business Objective #7)* ***Recommendation:*** TLC should work with IGT to perform periodic log reviews of DBA activity to ensure only authorized changes are being implemented. This may involve an amendment to the contract with IGT, to allow for a vendor audit or to specify that future SOC audits address the controls over database changes.	

Exhibit 2: Observation and Recommendation Summary.

BACKGROUND

The Lottery's largest contract is with International Game Technology (IGT). IGT Texas (TX) installs and manages the retailer equipment throughout the state and manages transaction processing systems (online gaming, administration, online gaming systems, and equipment) throughout the entire state. IGT TX also supplies various professional services, backup data processing, and the satellite communications network supporting gaming systems operations. The IGT TX systems are designed with the assumption that certain internal controls would be implemented by TLC. The application of such internal controls by TLC is necessary to achieve the control objectives identified. There are thirty (30) compensating controls listed in the IGT SOC report.

The agency's Information Resources (IR) division is responsible for implementing and monitoring software change controls. The agency's Information Technology Services Director oversees IR staff and activities.

TLC VENDOR SOFTWARE CHANGES BUSINESS OBJECTIVES, RISKS, FINDINGS AND MANAGEMENT RESPONSE

This section of the report provides a summary of applicable business objectives, risks, and controls in place to ensure that TLC's Vendor Software Changes are monitored, authorized, and tested by TLC prior to being placed in production.

Each table also includes our assessment of internal controls for the respective business risk, our recommendations to address deficiencies noted or opportunities to enhance current controls and management's response.

1 BUSINESS OBJECTIVE: IDENTIFY UNAUTHORIZED CHANGES	
Business Objective	To establish management controls that ensure the agency can identify unauthorized changes made to the IGT software as well as changes that are unsecured, or do not match what was requested.
Business Risk	➲ Changes may be made to the IGT software that are unauthorized, unsecured, or do not match what was requested.
Management Controls in Place	➲ The TLC Lottery Operator Software Changes policy and procedures details who is responsible for lottery operator software changes. ➲ According to IR, in the event a change does not match the request, users, IGT or customers will report the issue and the Incident Management Online (IMO) process is followed to resolve it. Emergency Bug Fixes are approved by TLC to be released into Production, but they do not undergo CAT.
Control Tests	➲ Interviewed key process owners. ➲ Reviewed Lottery Operator Software Changes policy and procedure. ➲ Sample tested to verify changes are authorized by TLC prior to implementation into production.
Control Assessment / Findings	**Internal Controls are Effective.**
Recommended Actions	None.
Management Response and Action Plan	None Required.

2 BUSINESS OBJECTIVE: CHECKSUM IDENTIFIES CHANGES	
Business Objective	To establish management controls that ensure reviews of checksum are completed and identifies all changes made to IGT program codes.
Business Risk	➲ Inability to track system changes through checksum can result in the production code being altered without an authorized program change.
Management Controls in Place	➲ Every software change performed by IGT is issued a checksum. Any changes to the checksum result in an automated email sent to the agency's Information Security Officer (ISO). ➲ The ISO also monitors the automated emails for checksum changes per procedures AD-IR-AA-007 IGT system change/access notification procedures.
Control Tests	➲ Interviewed key process owners. ➲ Reviewed IGT system change/access notification procedure.
Control Assessment / Findings	**Internal Controls are Effective. Some Improvement Opportunity for Documentation Retention.** ➲ Emailed reports associated with changes to main transactional engines, are not retained past 30 days unless a discrepancy is encountered. ➲ Five (5) of the five (5) sampled changes did not have evidence indicating the checksum change notification was sent to TLC.
Recommended Actions	TLC should retain notifications along with all artifacts\documents associated with the individual change.
Management Response and Action Plan	None Required.

3 BUSINESS OBJECTIVE: TESTING NEW SOFTWARE VERSIONS	
Business Objective	To establish management controls that ensure all IGT software changes are tested prior to being moved into the production environment.
Business Risk	➲ Testing new versions of software may not be completed prior to the code being placed into production.
Management Controls in Place	➲ Software changes are tested in CAT according to the approved requirements document. ➲ All requested changes in the requirement are tested by appropriate business users and IR staff. TLC staff work directly with IGT Quality Assurance (QA) staff to complete.
Control Tests	➲ Interviewed key process owners. ➲ Reviewed TLC Operator Software Test Planning. ➲ Reviewed TLC Software Development Life Cycle detailed acceptance testing document.

Control Assessment / Findings	**Internal Controls are Effective. Some Improvement Opportunity for Documentation Retention.** ➲ Approval of control testing performed to test financial transactions is informal and not documented. ➲ Two (2) of the five (5) sampled changes did not have evidence indicating the CAT test results performed by TLC.
Recommended Actions	1. TLC should retain the results of all CAT testing activity with all artifacts\documents associated with the individual change.
Management Response and Action Plan	None Required.

4 BUSINESS OBJECTIVE: PARTICIPATION IN CHANGE MANAGEMENT PROCESS

Business Objective	To design processes that ensure TLC responsibilities are met regarding its participation in IGT system modification requests, including CAT and approval of specifications and final approval of completed changes, is performed by appropriately authorized personnel.
Business Risk	➲ Participation in IGT system modification requests may not be performed at all or may not include appropriately authorized personnel.
Management Controls in Place	➲ IGT and TLC have a joint agreement on items that require prior approval. These items are outlined in the Changes Requiring TLC approval V2.2. According to the document, IGT must submit a formal approval request prior to making any change(s). ➲ The agency maintains a list of authorized TLC personnel that may provide written approval of request for change and list of authorized IGT personnel that may submit request for change to TLC.
Control Tests	➲ Interviewed key process owners.
Control Assessment / Findings	**Some Improvement Needed.** ➲ It was noted that there is no formal approval process of CAT completion by the agency's associated departments\business owners. ➲ Weekly meetings with TLC business owners (major release) usually have an agenda is in place, but no minutes are maintained. ➲ Multiple artifacts associated with an individual change are not maintained in a centralized location. This would include the following: • Formal approvals from the business owners. • The test case spreadsheet.
Recommended Actions	1. TLC should retain the results and approvals associated with CAT testing activity with all artifacts\documents associated with the individual change for the required three (3) year retention period. 2. TLC should retain all artifacts\documents associated with individual changes in a centralized location, such as the agency's document repository system.

4 BUSINESS OBJECTIVE: PARTICIPATION IN CHANGE MANAGEMENT PROCESS	
Management Response and Action Plan	TLC agrees with the recommended actions. The changes have been implemented; all approvals, documents and communications related to IGT software changes are saved in Teams in a centralized location.

5 BUSINESS OBJECTIVE: TLC CUSTOMER ACCEPTANCE TESTING PROCEDURES& SYSTEM CHANGE APPROVALS	
Business Objective	To ensure TLC responsibilities for managing CAT procedures and the approval of CAT system changes.
Business Risk	➲ Customer Acceptance Testing (CAT) may not be managed to assure proper approval of system changes.
Management Controls in Place	➲ IGT coordinates with TLC when a refresh of the CAT environment is necessary. ➲ TLC manages access\roles to the CAT environment for TLC testing personnel. ➲ In the event of an Emergency Bug Fix TLC relies on the testing performed by IGT. This will ultimately result in a refresh of the CAT environment.
Control Tests	➲ Interviewed key process owners.
Control Assessment / Findings	**Some Improvement Needed.** ➲ IGT is not required to obtain TLC's approval to refresh CAT. However, they do coordinate with TLC when a refresh is necessary. ➲ An Emergency Bug Fix testing process is not formally documented. ➲ There is not a formal process ensuring business owners perform post implementation testing.
Recommended Actions	1. TLC should formally document and retain evidence of approval associated with the refreshing of the CAT environment by IGT. 2. TLC should work with IGT to formally document the Emergency Bug Fix process. 3. TLC should maintain a log of all EBFs, including the reason associated with the EBF. 4. TLC should update the Testing of Program Modifications AD-IR-SO-024 procedure to include specific requirements associated with post implementation testing by the business owner.
Management Response and Action Plan	TLC agrees with the recommended actions. The following items were implemented: • TLC updated the "Changes Requiring TLC Approval" document to include the CAT refresh. A draft of document was sent to IGT for approval. Upon execution of the document, IGT will be required to formally request TLC's approval to refresh CAT. TLC will retain approvals in Teams in a centralized location. • The EBF process requires formal approval from TLC. TLC will retain approvals in Teams in a centralized location.

5 BUSINESS OBJECTIVE: TLC CUSTOMER ACCEPTANCE TESTING PROCEDURES& SYSTEM CHANGE APPROVALS	
	• TLC updated the Testing of Program Modifications AD-IR-SO-024 procedure to include specific requirements associated with post implementation testing by the business owner.

6 BUSINESS OBJECTIVE: COMMUNICATION METHODS	
Business Objective	To design management controls that determine the communications method utilized to connect to IGT TX's systems (e.g., direct connections, over public networks, etc.).
Business Risk	➲ Communication methods utilized to connect to IGT TX's systems may not be authorized, secured, or drop transmissions.
Management Controls in Place	➲ The TLC contract with IGT indicates the critical functions which IGT must provide, such as redundancy of connectivity. ➲ Changes to the network and communication protocols are managed within the IGT Request for Change (RFC) process, with TLC providing approval prior to implementation. ➲ The TLC ISO performs an annual review of the IGT San Antonio Backup data center. ➲ On an annual basis, TLC and IGT conduct a review of the Network infrastructure\diagram to verify connectivity in secure zones.
Control Tests	➲ Interviewed key process owners. ➲ Reviewed the 2018 Multi-State Lottery Association (MUSL) report**.** ➲ Reviewed the 2020 MUSL review of the IGT San Antonio backup data center.
Control Assessment / Findings	**Internal Controls are Effective.**
Recommended Actions	None.
Management Response and Action Plan	None required.

7 BUSINESS OBJECTIVE: IGT DATABASE CHANGES	
Business Objective	To determine if changes implemented by the IGT database administrators (DBAs) are authorized, and IGT maintains logging of DBA activity.
Business Risk	➲ IGT personnel may make changes directly to the database without prior approval.

7 BUSINESS OBJECTIVE: IGT DATABASE CHANGES

Management Controls in Place	➲ The agency's Information Security Officer (ISO) receives alerts when an IGT Engineer or DBA has access elevated to perform changes in the production environment. ➲ The automated system access notification (email) does not show the actual changes; however, the activity is logged (MUSL requirement), which IGT can review to ensure changes were appropriate.
Control Tests	➲ Interviewed key process owners.
Control Assessment / Findings	**Some Improvement Needed.** ➲ TLC does not have insight into all activity performed by IGT DBAs and must rely on IGT internal controls for monitoring and logging of all DBA activity, to ensure changes by DBAs are authorized.
Recommended Actions	TLC should work with IGT to perform periodic log reviews of DBA activity, to ensure only authorized changes are being implemented. This may involve an amendment to the contract with IGT, to allow for a vendor audit or to specify that future SOC audits address the controls over database changes.
Management Response and Action Plan	TLC does not agree with the recommendation for two reasons; review of the very voluminous logs will require resources that TLC does not have available and since the retention period of logs is so short the periodic review would have to happen monthly at a minimum. TLC has decided to adopt an alternative method of implementing an annual security review of who has the security credentials to allow for direct modification to the database and review any changes made by such individual. TLC will work with the vendor on the annual review to implement the alternative method.