



**TEXAS LOTTERY
COMMISSION**



An Internal Audit of Texas Lottery Commission Active Directory

August 25, 2017

Report #17-009



McCONNELL & JONES LLP
CERTIFIED PUBLIC ACCOUNTANTS

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.



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 Active Directory user access control environment. We conducted this audit 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 provides a reasonable basis for our observations and conclusions based on our audit objectives.

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.

Objectives and Scope

The purpose of the audit is to review the Texas Lottery Commission’s user management and administration of the Active Directory ensuring risk management and compliance with the system access control guidance outlined in Texas Administrative Code 202.

We examined the following process during the audit:

1. TLC’s progress in addressing items noted in the FY 2016 security study report issued in September 2016.
2. General management of the agency’s Active Directory (policy and procedures).
3. Information system access request procedures.
4. Network and information system access rights creation, maintenance and termination.
5. Management of network and information system user rights.

The audit scope was from September 1, 2015 – March 31, 2017.

Results and Conclusion

The internal controls governing the user management and administration of the agency’s Active Directory are effective and working as intended to achieve the business objectives and compliance with regulatory requirements. TLC’s processes for managing the active directory are best practices. Our audit work identified no reportable findings.

| Rating | Description of Ratings |
|-------------------------|---|
| 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. |
| 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 | A few specific control weaknesses were noted; generally however, controls evaluated are adequate, appropriate, and effective to provide |



| Rating | Description of Ratings |
|--------------------------|---|
| Major Improvement Needed | <p>reasonable assurance that risks are being managed and objectives should be met.</p> <p>Numerous specific control weaknesses were noted. Controls evaluated are unlikely to provide reasonable assurance that risks are being managed and objectives should be met.</p> |
| Unsatisfactory | <p>Controls evaluated are not adequate, appropriate, or effective to provide reasonable assurance that risks are being managed and objectives should be met.</p> |

Acknowledgement

We wish to thank all staff involved in this audit for their professionalism and positive outlook

towards the assessment of the agency's Active Directory management. The timely completion of this audit was due to their efforts and responsiveness to our requests.



Active Directory is the database that facilitates connectivity and user access to interconnected network resources and data. Active Directory authenticates and authorizes individual's access.



Executive Summary

The section of the report provides a summary of Texas Lottery Commission's Active Directory user management and administration internal control environment based on audit procedures. We noted the Texas Lottery Commission's internal controls for key process related to user management and administration are effective and working as intended.

Active Directory is a database system developed by Microsoft and used in Microsoft Windows environments. Active Directory stores information about network components and facilitates working with the interconnected network resources. The main

purpose of the Active Directory is to provide central authentication and authorization services for Microsoft Windows based computers. Active Directory is an effective way to manage all elements of the agency's network including computers, groups, users, domains, security policies and user-defined objects. The Active Directory information and setting are stored in a central database.

Figure 1 provides an illustration of high-level generic Active Directory environment and documents how the data owners, data information and applications interact to facilitate the agency's network component access.

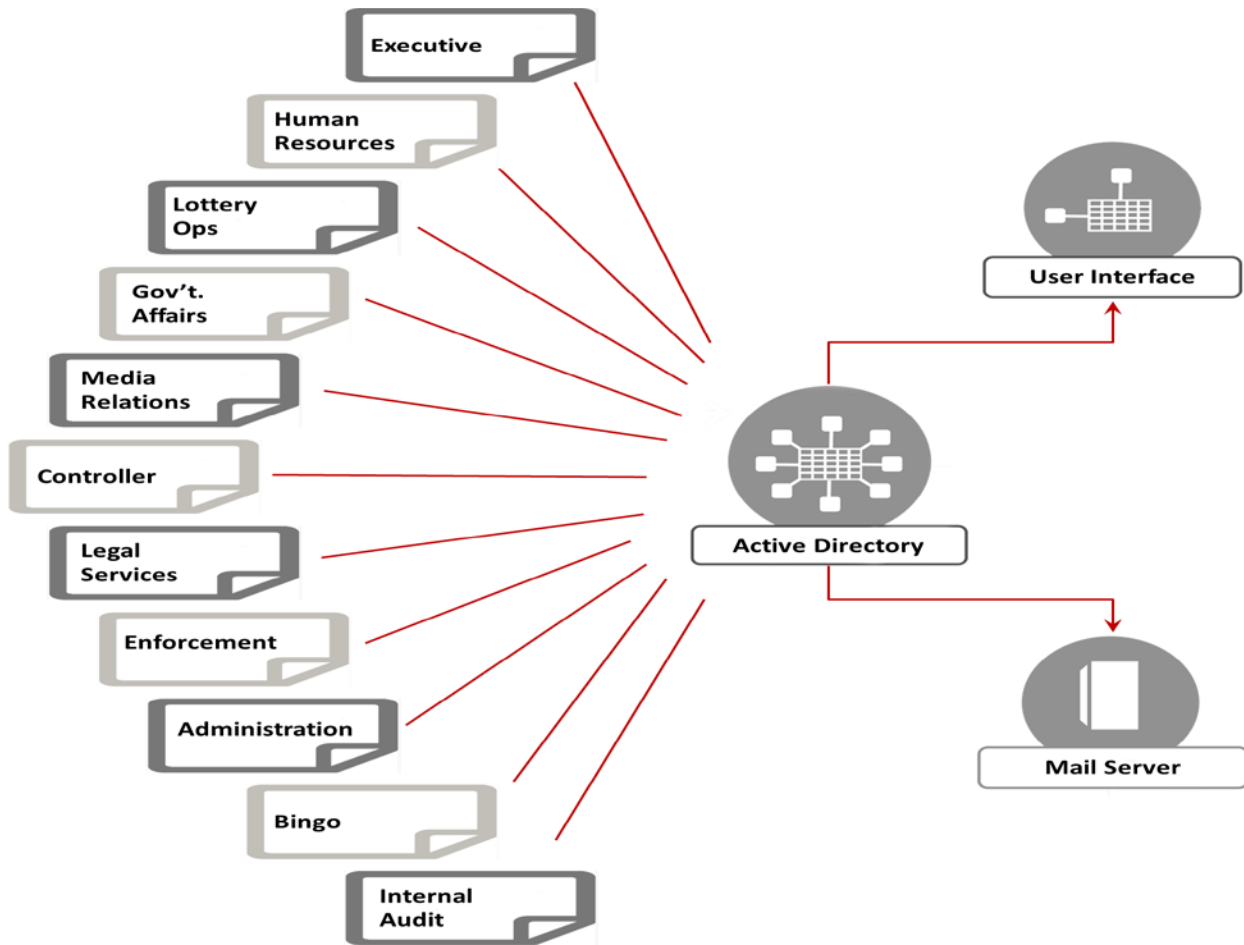


Figure 1: Active Directory Overview



The following tables describe the Texas Lottery Commission’s Active Directory user

management and administration processes and controls.

BUSINESS OBJECTIVE 1: Addressing Audit Findings

| | |
|-------------------------------|---|
| Business Objective | Texas Lottery Commission management team takes necessary action to effectively address audit findings and ensure management of risk exposures. |
| Business Risk | Audit findings not effectively addressed to ensure management of risks associated with the agency’s Active Directory. |
| Management Controls | ➤ Management addressed two findings related to Active Directory noted in the FY 2016 security study. |
| Control Tests | ➤ Reviewed Active Directory password settings. ➤ Conducted interviews with management and staff. |
| Control Environment | Effective The following documented findings were in the FY 2016 security study report issued in September 2016 and the corrective actions taken. Low Risk Finding: Active Directory security parameter for minimum passwords age was set to “0” days allowing immediate resetting of passwords. Corrective Action: Setting changed to a minimum of 3 days as noted by the audit recommendation. Low Risk Finding: Passwords not meeting Agency policy. Corrective action: Review of the exceptions to the policy completed and approved by the IT manager and Administration Director. |
| Recommended Actions | None |
| Management Action Plan | None required |

BUSINESS OBJECTIVE 2: Active Directory Policy and Procedures

| | |
|----------------------------|--|
| Business Objective | Texas Lottery Commission governs Active Directory user management and administration through established policies and procedures that address the authority, roles and responsibilities of key process owners. |
| Business Risk | The agency’s data owners do not understand the process to ensure access to data information is provided based on individual’s roles, responsibilities and needs. |
| Management Controls | ➤ Policies and procedures have been developed to ensure staff have an understanding of how data owners can gain access to information and applications. ➤ Policies and procedures are reviewed and updated as per the agency’s policy and procedure management process. |



BUSINESS OBJECTIVE 2: Active Directory Policy and Procedures

| | |
|-------------------------------|---|
| | <ul style="list-style-type: none"> ➤ Mature understanding and size of the agency reduces the risk exposure of giving access without proper review from data owners and IT administration. |
| Control Tests | <ul style="list-style-type: none"> ➤ Conducted interviews. ➤ Reviewed policies and procedures. ➤ Tested for compliance with TLC policies, procedures and system access control section of Texas Administrative Code 202. |
| Control Environment | Effective |
| Recommended Actions | None |
| Management Action Plan | None Required |

BUSINESS OBJECTIVE 3: User Accounts Provisioned and Terminated

| | |
|----------------------------|---|
| Business Objective | To ensure that the agency has developed processes ensuring provisioning and termination of user are requested, reviewed, and approved with documentation. Users have rights in accordance with business functions. (Need to Know basis) |
| Business Risk | No formal process to govern Active Directory access, which creates risks to the management of the agency's applications and data information. |
| Management Controls | <ul style="list-style-type: none"> ➤ Agency has developed an Information Service Request (ISR) system used by the department heads (data owners) to manage access to applications and data / information. ➤ Agency department heads and designated managers are the agency's data owners with the proper authority to request access to data / information and applications. ➤ Policies and procedures govern how the ISR process is to be completed. ➤ ISRs require approval from IT administration to ensure proper access is given. ➤ Information Security Officer coordinates with the division heads to complete an annual review of access rights with adjustments completed and documented through the ISR process. |
| Control Tests | <ul style="list-style-type: none"> ➤ Conducted interviews. ➤ Performed walkthroughs. ➤ Reviewed policies and procedures. ➤ Tested ISR and user access. |
| Control Environment | Effective |



BUSINESS OBJECTIVE 3: User Accounts Provisioned and Terminated

Recommended Actions None

Management Action Plan None required

BUSINESS OBJECTIVE 4: Password Policy and Authentication

Business Objective To ensure that the Texas Lottery Commission has established protocols for authentication as it pertains to passwords.

Business Risk Password standards are not maintained by the agency to ensure proper data / information security.

Management Controls

- Active Directory has established criteria for password management.
- The current Active Directory setting meets best practice standards for password management.
- A review of user access is completed on an annual basis by the agency's Information Security Officer.

Control Tests

- Performed walkthroughs.
- Conducted interviews.

Control Environment Effective

Recommended Actions None






Management Action Plan None required



Texas Lottery Commission Internal Controls Environment

The Texas Lottery Commission developed and instituted an effective control environment that aligns with the agency’s data security

requirements. The chart below reflects the key controls and respective control rating based on the audit procedure applied.

| Internal Controls Practices | Rating |
|--|---|
| Risk-based policies and procedures that include defined roles, authority and responsibilities are developed and maintained. |  |
| Texas Lottery Commission’s information system access controls are compliant with State Statute. |  |
| Information Service Request (ISR) application allows the data owners (department heads and designees) to work with Information Resources to ensure proper data access. |  |
| Annual application reviews ensure user access provided to employees is based upon the need for data / information or application based on job duties. |  |
| Password management and integrity rules have been established and maintained. |  |