April 23, 2023 Report No. [01-01]

Mr. Dejuan Ross, Vice President

**Audit Report: Oracle Database Administration**

We have completed an audit of the Oracle Database Servers for which fieldwork began March 10, 2023. Our audit was directed towards determining whether proper controls are in place within the database to prevent breaches of security, limit user access based on permissions, and logging/monitoring changes in the database. The audit was conducted in accordance with the Institute of Internal Auditors’ *International Standards for the Professional Practice of Internal Auditing.*

The scope of our audit included a complete review of the current controls over the availability and security of the Oracle database servers. Within this review, we focused on ensuring that the security controls in place mandated password parameter settings and password complexity. We also focused on making sure that there are proper controls in place to limit crucial privileges from being given to unauthorized users. Additionally, our audit scope included the investigation into the segregation of testing and production databases. We reviewed that a segregation exists, and validated if it is adequate, and that changes done in the testing database would require approval from privileged users before being launched into production database. Furthermore, the scope of our audit included a review of the controls in place to log and monitor data that is stored in the database. These tests included verifying whether or not the data is stored and encrypted properly, assuring that unnecessary data is not being collected, and that the data has a retention period specified in the records management. We also performed other audit procedures as deemed necessary to ascertain the degree of compliance with applicable laws, regulations, established policies and procedures, and to determine, where practical, if improvements and efficiency in operations could be gained.

Based on the results of our audit, we formed the opinion that there is a need for improvement within the database system: the internal controls need improving and operations are not in sufficient compliance with policies, procedures, laws or regulations. The report includes violations, weaknesses, unsafe or unsound practice or conditions, exceptions and recommendations. The controls that are in place do not efficiently mitigate the risks that are present in the database. Our testing of controls revealed a number of opportunities for improving efficiency.

We determined that aside from the issues described above, the database server has sufficient encryption of sensitive PII data of customers and that there is adequate segregation between testing and production servers. We have also determined that the production database server is properly safeguarding users from applying changes to it without going through an authorized user’s approval process. Lastly, we have verified that database versions are properly up to date, and that there is a proper retention period specified in the records management that follows compliance.

We concluded that controls and procedures over the availability and security of the Lexus Oracle database **"Needs Improvement”**. While there are proper controls set in place for the encryption of PII data, the segregation of testing and production databases, and the logging of internal data, there is a glaring lack of controls in other parts of the database system. The controls in place for ensuring proper password parameters are not compliant with information security baseline standards. The controls in place for ensuring that users who are not privileged to write/edit the database are improperly configured. The controls in place for both employee onboarding and termination are inadequate. Lastly, the controls in place for documenting and approving changes in the database also need improvement.

Due to the pending status of the corrective action(s), we will follow-up on the open finding(s) and periodically report the status to senior management and the Audit Committee. If you have any questions, we will be pleased to discuss them with you.

Auditor-In-Charge: Austin Reaves, CIA, CISA, CGEIT

Respectfully submitted,

Austin Reaves, CIA, CISA, CGEIT

Vice President, Information Technology Audit Manager

Elliot Alderson, CPA, CBA, CFE, CFSA, FCPA

Senior Vice President, Chief Audit Officer

cc: Board of Directors

Mr. Dejuan Ross, Vice President, Associate General Counsel – Compliance

Mr. Andy Samberg, Senior Vice President, Chief Information Officer

Mr. Tom Petty, Vice President, Director of IT Risk Management

Mr. Logan Roy Manager of IT Governance Risk and Compliance

*This report and its attachments are the property of the Lexus and are for its confidential use.  Access is limited to members of the board and those officers and employees of Lexus whom the chief audit officer determines have need for such access, the Lexus external auditors.  Under no circumstances shall any individual or entity to whom access has been provided disclose in any manner this report or any portion thereof to any person or organization not officially connected with Lexus as officer, director, employee, external auditor, or regulator without authorization from the chief audit officer.*

**Summary of Findings**

|  |  |  |
| --- | --- | --- |
| **Unsafe or Unsound Practice or Condition Number** | **Unsafe or Unsound Practices or Conditions** | **Expected Date of Implementation** |
| 1. | A new employee was given access to the database without taking appropriate approvals. | May 30, 2023 |
| 2. | Password parameter settings for employees in the Oracle database account is not in compliance with information security baseline standards. | June 30, 2023 |
| 3. | All the users having access to the database have a "Write" access to it, hence, any user having the access to database production, can make changes to it. | September 30, 2023 |
| **violation**  **Number** | **violations** | **Expected Date of Implementation** |
| 1. | An employee who had administrator privileges left the company, however, his database login credentials were not revoked. | September 30, 2023 |
| **WEAKNESS**  **Number** | **WEAKNESSES** | **Expected Date of Implementation** |
| 1. | Changes to the database system are not documented in a ticketing system and formal approvals are not obtained. | September 30, 2023 |
| 2. | The audit log of database user activities is not reviewed. | June 30, 2023 |

|  |  |
| --- | --- |
| **Unsafe or Unsound Practice or Condition Number** | **Recommendations** |
| 1. | It is advised to develop automated workflows for the Identity Management form approval process to address the issue of incorrect access provision to the database. To limit potential risks, managers and application owners should be trained on the importance of adhering to the proper approval process. There should be an "Approval Flow Policy" in place. Regular audits should be done to ensure compliance. |
| 2. | To address the audit findings regarding non-compliant password parameter settings in the database, it is recommended to review and update the current password policies and ensure that they comply with the established information security baseline standards and as per the company guidelines. Password complexity requirements should be enforced, including length and complexity requirements, and periodic password expiration should be implemented based on the parameters set by the company. |
| 3. | To restrict unauthorized access to the production database, Role based access controls will be implemented that restrict users from making any changes to the database. Like “Write” Access should be only given to people who are doing the implementation. Admin access should be limited to authorized personnel and should be monitored and reviewed on a regular basis. A user access review should be introduced which involves periodically reviewing access rights for all an organization's employees and third parties. |
| **violation**  **Number** | **Recommendations** |
| 1. | It is advised that a proper exit management system needs to be in place to swiftly revoke access for the terminated personnel to address this problem. All database accounts connected to the terminated employee should be reviewed as part of this procedure, including any privileged accounts, and disabled. JML or a Joiner-Mover-Leaver phase should be introduced to ensure proper exit for the employee. All access should be revoked on the first day itself. Access Revoke emails should be sent to the employee within a 48-hour window of his termination. |
| **WEAKNESS**  **Number** | **Recommendations** |
| 1. | To solve the problem of erroneous access provision to the database, it is advised to create a ticketing system workflow that can be introduced in place to for approvals. An entire "Approval Flow Policy" should be put into place based on the ticketing system where changes should be going for approval to the authorized personnel and tickets will be generated based on that. Audits should be conducted often to ensure compliance. |
| 2. | The audit logs of database user activities should be regularly checked to make sure that the users who have access to the database are not doing anything they shouldn't be doing. A control system should be in place to alert the DBA staff if the audit logs are not being recorded. This will help ensure that the database is being used appropriately and that unauthorized activities are caught and addressed in a timely manner. |