**CIS Class Audit**

**Internal Audit Division**

**TEAM : LEXUS**

**Draft Finding Sheet**

**April 23 2023**

1. **A new employee was given access to the database without taking appropriate approvals.**

A new employee’s access should be provisioned on the basis of appropriate approvals. A ticketing system should be in place to complete the process, the request should be raised by the HR and approval from the line manager, or the CIO should be taken to grant access. The request should include the type of access requested.

As per the company policy, only the Oracle DBA team should have access to the database. The same should be provisioned upon getting approvals from the technology manager.

In case the provisioning does not happen basis the approvals, it can cause unauthorized access creations and unauthorized activities can take place.

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.

**Responsible Manager:** Mr. Jane Doe

**Management Response:** It was noted that it was only one sample with this issue and the others complied with the policies in place. Further, it was identified that it was an authorized user and access provisioned was correct.

**Targeted date of implementation:** May 30, 2023

1. **An employee who had administrator privileges left the company, however, his database login credentials were not revoked.**

When an employee leaves the company, it is usually a good practice to raise a request of revocation well in advance. It is advised that the line managers initiate the request and then the HR confirms and moves it forward.

As per the company policy, access is required to be revoked within 48 hours of employee’s last working day. This includes revoking his physical access to the premises along with the logical access to the databases and applications he has access to.

In the above identified issue, it was noted that the user left the company on January 9th, 2023 and his account was revoked on Feb 3rd, 2023. The time to suspend his account was more that 3 weeks which left the company at a major risk as the account owner had administrator privileges. Unauthorized activities could have been carried using this account without holding anyone accountable for the same.

It is advised that a proper exit management system needs to be in place to swiftly revoke access for the terminated personnel in order 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 in the first day itself. Access Revoke emails should be sent within a 48-hour window of his termination.

**Responsible Manager:** Ms. Julia Davis

**Management Response:** The exception was identified for only user account and upon performing the remediation testing, it was noted that the user account was last logged in on the last working day of the employee. Hence, no activities were performed from it.

**Targeted date of implementation:** April 30, 2023

1. **Password parameter settings for employees in the Oracle database account is not in compliance with information security baseline standards.**

It is usually good practice to have a password policy which baselines the security parameters for each application and AD in use. This should be reviewed annually to be in line with the changing password methodologies.

As per the company policy for Oracle database, the minimum password length should be 12 characters and the complexity should be enabled for the same.

In the exception noted for the administrator account, we identified that the password length and complexity criteria was not enabled in Oracle system. Having a weak password set for a strong account can put the company at risk of being attacked easily.

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.

**Responsible Manager:** Mr. Scott Cameron

**Management Response:** The exception noted is for the administrator account and the settings for the password configuration were kept as per the default settings in Oracle. The team will align the same as per the company’s Information Security Policy.

**Targeted date of implementation:** June 30, 2023

1. **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.**

It is usually a good practice to limit role provisioning basis the need of access. If a user does not require a “write” access, his access should be limited to “read” only.

The Information Security Policy does not mention access management using role-based access configurations. This should be a process improvement for the firm and role-based access provisioning should be made.

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 a 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 of an organization's employees and third parties.

**Responsible Manager:** Ms. Lucia Wang

**Management Response:** This has been noted as a process improvement and role-based access provisioning will be implemented going forward at the end of Q3.

**Targeted date of implementation:** September 30, 2023

1. **Changes to the database system are not documented in a ticketing system and formal approvals are not obtained.**

Internal audit recommends having an external ticking tool where approvals are obtained and documented along with the results for UAT. This can help streamline the process and prevent implementation of unauthorized changes in the system.

It was noted that the current process includes taking approvals over emails and then performing the implementation on the systems. The changes are logged in the tool, however, review of changes done is not performed.

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.

**Responsible Manager:** Mr. Jeremy Warren

**Management Response:** Management noted the same and will be implementing a ticketing tool at the end of Q3. However, no inappropriate changes were made during the review period. As part of remediation testing, management reviewed the changes done and no issues were identified.

**Targeted date of implementation:** September 30, 2023

1. **The audit logs of database user activities are not reviewed.**

Audit logging is important for database security because it provides a way to monitor and record all activity that occurs within a database. This includes not only database modifications, but also access attempts, logins, and other system events. By recording all of this information, audit logs can be used to detect and investigate potential security breaches, as well as to identify patterns of suspicious behavior that might indicate an attempted attack or other unauthorized activity. This information can also be used to track user activity and identify any compliance or regulatory violations.

Internal audit noted that the log activities in the database were recorded as logging is enabled, however, a timely review of the logs should be in place to make sure that inappropriate changes are not bi passed and stay in the system.

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.

**Responsible Manager:** Mr. Juan Ordonez

**Management Response:** Management noted the issue and will be performing a quarterly review of the changes going forward. It was also noted in the remediation testing that a log does get generated in the backend however, the same is not reviewed for appropriateness. The same will be remediated starting Q3.

**Targeted date of implementation:** June 30, 2023