Croydon Council General Purposes & Audit Committee – IT Controls in My Resources

Victoria Richardson
Head of HR & Finance Service Centre
Resources Department

Purpose of the Presentation

1. To update members on progress towards addressing the Oracle security and access controls findings from the 2019/20 IT Controls Audit.

Deficiency 1 - Segregation of duties conflicts between Oracle system administration, developer, and finance roles

Recommendation

The recommendation from the Auditors was for management to consider reviewing the elevated access assignment and, where possible, restricting Oracle administrator access to members of the IT department only with all conflicting finance responsibilities being removed from System administrator accounts.

Update

- We found that system admin access was assigned to system accounts or members of the support and implementation teams.
- We have ended the implementation team user accounts
- We have reduced the number of people with system admin accounts
- Effectively monitoring segregation of duties manually is time consuming and cannot be done with office tools. We are considering the business case to use Oracle Risk Management Cloud, which can implement appropriate formalised and documented controls to monitor system administrator and support team access as a tool is required analyse and monitor.
- In the interim, we are investigating the use reports to provide some limited monitoring of system administrator and support team access

Deficiency 2 – Oracle system configuration access granted to an excessive number of users, including non-IT staff / end users

Recommendation

Management should consider reviewing all users with system configuration capabilities assigned and, where possible, removing this from end users / limiting this access to members of IT department.

Update

- The relationship between roles and privileges is complex, we have engaged our support provider, to help us assess the risk posed by the privileges and recommend appropriate actions.
- We completed a detailed piece of work to understand where system configuration privileges exist within roles assigned to users outside of the support team. This identified a number of users where the configuration privileges assigned are appropriate for their role e.g. HR Data Team setting up new positions for staff.
- Some users have been allocated roles with specific configuration privileges inherent within them. The configuration privileges are not required for their day to day work. We have undertaken sample testing to confirm if users can perform system configuration changes using that privilege. The testing confirmed that they do not have access via the application. This is because access depends on a number of complimentary controls e.g. security profiles, data roles. Our analysis indicates that in these cases the risk may be reduced. For completeness, we are investigating if we can create a role with the configuration privileges remove.
- We have removed configuration privileges from users identified in our analysis where it was low impact and simple to address.

Deficiency 3 - Users self-assigning responsibilities without formal management approval

Recommendation

Where administrative staff require additional functionality, they should be required to request this through the formal change management procedures.

.

Update

- We have identified that there has been self-assignment of forecast approver roles within the projects module by project managers. We have reviewed the controls and are working on a solution to prevent this.
- We have removed the ability for third-party support team members to assign responsibilities. Access will be given as & when required and monitored so it and removed when no longer needed.
- We have now removed access to the IT security manager role from 3rd Party support staff.
- The majority of self-assignment occurred during or just after implementation, however we have restated the message that that the internal My Resources support team must not self-assign roles and must follow the normal user access request process if they require additional responsibilities.
- We are developing monitoring controls via a report to identify instances where members of staff have assigned themselves additional responsibilities and any non-compliance.

Action Plan – Appendix A - Oracle Cloud IT Controls Audit
Action Plan June 2021

Auditors Summary

Questions

Thank you

Victoria Richardson
Head of HR & Finance Service Centre
Resources Department