Croydon Council Audit and Governance Committee – IT Controls 2022/23

Jon Martin

Interim Head of Strategic Systems

Assistant Chief Executives Department

14th March 2024

Purpose of the Presentation

1. To update members on progress towards addressing the security and access controls findings from the 2022/23 IT Controls Audit for Oracle Fusion (‘My Resources’) and NEC Revenues & Benefits IT systems.

Oracle Fusion Update

Point 1 – Inappropriate elevated privileges in business process roles in Oracle Fusion

Recommendation

Management should consider reviewing the five identified business roles with elevated privileges to remove any risk of them having unauthorised and unnecessary access to sensitive data.

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.
- Within Fusion, the access security architecture is notably complex. It's crucial to recognize that beyond just roles and privileges, other controls are in place dictating the level of access to functionality and icons for users. In light of this complexity, we have engaged our support provider to assist in assessing the risks associated with privileges and recommending appropriate actions.
- Following a thorough analysis of the roles and privileges, our support partner has confirmed the complexity and challenges associated with removing all privileges linked to those roles without affecting core functionalities. Consequently, we have implemented workarounds to ensure that business process roles cannot access potentially sensitive data. This involves disabling relevant icons that grant access, while still keeping them available for support team members who require them.
- During the audit, this deficiency was categorized as a "Red" issue. However, we believe that the mitigations currently in place have significantly alleviated its impact. We are actively engaging in discussions with the auditors to ensure that we are providing the necessary evidence to demonstrate this improvement.
- As a recommendation, our Support Partners have suggested implementing Oracle Risk Cloud, which includes modules such as Advance Access Control. This facilitates real-time monitoring of sensitive privileges and offers additional functionalities like Access Certification and Access Request Approval Workflow
- The Oracle Risk Cloud module is included in the scope of the finance workstream of the Oracle Improvement Programme. This will provide tools and dashboards to help monitor this area. It is expected to be implemented by 31st Dec 2024.

Point 5 – Lack of audit logging in Oracle Fusion

- Some audit logging capabilities (e.g., capturing additional events) may have an adverse impact on system performance. We feel the better initial route is to explore the Oracle Risk Cloud suite of tools.
- The Oracle Risk Cloud module is included in the scope of the finance workstream of the Oracle Improvement Programme. This will provide tools and dashboards to help monitor this area. It is expected to be implemented by 31st Dec 2024.
- Upon integration, we expect this module to greatly enhance audit logging, especially in critical financial areas, ensuring more detailed monitoring and compliance measures.

NEC Revenues & Benefits Update

Point 8 – Lack of third-party IT assurance reporting for NEC – Revenues & Benefits

- This is noted and accepted, we will be initiating the conversations.

Point 9 – Lack of review of audit logs in NEC – Revenues & Benefits

- User actions of officers are monitored by team managers in the performance reporting, their log in time is also part of that performance reporting. Users have access defined by their roles and it would not be unusual for any officer to be taking any action they have the permissions to take. There are checks and balances in place to make sure that the system is operating as it should be and no user would be able to take unnoticed action. The system cannot be brute forced for entry, 3 repeated password failures end in a lockout for that user, there is no timeout between attempts that resets that.

Point 10 – Weak password setting for NEC – Revenues & Benefits

- This change is a time-consuming process as each user needs to go through a password reset process and initially this password needs to be set by an administrator. We tackled this team by team and most of this process had been complete at the time of the audit. Since this review, we have now finished this process all current users are now migrated to an LBC_* profile.

Auditors Summary

Questions

Thank you

Jon Martin
Interim Head of Strategic Systems
Assistant Chief Executives Department