Public Document Pack

Audit & Governance Committee Supplementary Agenda

13. **I.T Control Audit Report** (Pages 3 - 32)

A presentation will be given to update the committee on the progress with IT Controls Audit 2022/23, slides attached at **Appendix A**. Appendix B is exempt under paragraph 3 of Schedule 12A of the Local Government Act 1972 and sets out the audit findings in full in respect of the IT Controls Audit 2022/23.

For the reasons set out in the report and its appendices, Audit & Governance Committee are recommended to:

Receive the presentation and update on IT controls.

Katherine Kerswell
Chief Executive
London Borough of Croydon
Bernard Weatherill House
8 Mint Walk, Croydon CR0 1EA

Hannah Cretney, Democratic Services
020 8726 6000
hannah.cretney2@croydon.gov.uk
www.croydon.gov.uk/meetings

This page is intentionally left blank

LONDON BOROUGH OF CROYDON

REPORT:	**Audit & Governance Committee**	
DATE OF DECISION	**14th March 2024**	
REPORT TITLE:	**Update on IT Controls Audit 2022/23**	
CORPORATE DIRECTOR / DIRECTOR:	**Jane West, Corporate Director of Resources and Section 151 Officer**	
LEAD OFFICER:	**Jon Martin, Interim Head of Specialist Systems** **Email: jon.martin@croydon.gov.uk**	
LEAD MEMBER:	**Cllr Jason Cummings, Cabinet Member for Finance**	
CONTAINS EXEMPT INFORMATION?	**YES**	**Public with exempt Appendix B.** Exempt pursuant to Paragraph 3 of Schedule 12A of the Local Government Act 1972 (Information relating to the financial or business affairs of any particular person (including the authority holding that information)) It is considered that in all the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosing the information.
WARDS AFFECTED:	**All**	

1 SUMMARY OF REPORT

1.1 A presentation will be given to update the committee on the progress with IT Controls Audit 2022/23, slides attached at **Appendix A**. Appendix B is exempt under paragraph 3 of Schedule 12A of the Local Government Act 1972 and sets out the audit findings in full in respect of the IT Controls Audit 2022/23.

2 RECOMMENDATIONS

For the reasons set out in the report and its appendices, Audit & Governance Committee are recommended to:

2.1 Receive the presentation and update on IT controls.

3 REASONS FOR RECOMMENDATIONS

3.1 This report and presentation provide an update for Audit and Governance Committee.

4 BACKGROUND AND DETAILS

4.1 Part of the scope of the external audit is to review the IT Controls in place for agreed key systems. Whilst incorporated into the overall auditor's submission for each financial year, the specialist nature of the IT Controls warrants a separate report and discussion.

4.2 The agreed in scope key systems are:

4.2.1 Oracle Fusion – the platform used to deliver the council's 'My Resources' solution covering finance, HR, payroll, and procurement functions.

4.2.2 NEC Revenues and Benefits.

4.3 The presentation at **Appendix A** covers the IT Controls Audit 2022/23 findings, work done to date, and priority areas to address.

5 CONSULTATION

5.1 This report and its appendices provide an update on the work being undertaken to mitigate concerns identified by the external auditor. There is no requirement for Member or Public consultation.

6 CONTRIBUTION TO COUNCIL PRIORITIES

6.1 The scope of this report covers two of the council's critical business systems. It's focus on assuring effective controls over use and access to these systems means it is part of the mayor's priority to *ensure good governance is embedded and adopt best practice.*

7 IMPLICATIONS

FINANCIAL IMPLICATIONS

7.1 As this is an update report for noting, there are no financial considerations directly arising from this report.

7.2 Comments approved by Lesley Shields, Head of Finance for Assistant Chief Executive and Resources on behalf of the Director of Finance. 06/03/2024

LEGAL IMPLICATIONS

7.3 There are no direct legal implications arising from the recommendations in this report. Members will, however, be aware that the Council as a best value authority "must make arrangements to secure continuous improvement in the way in which its functions are exercised, having regard to a combination of economy, efficiency and effectiveness"

(Section 3 Local Government Act (LGA) 1999). The Best Value Duty applies to all functions of the Council.

7.4 On 20th July 2023, the Secretary of State for Levelling Up, Housing and Communities ("the SoS") issued Directions under Section 15(5) of the LGA to the Council on the on the basis that the Council was failing to comply with its Best Value Duty and setting out actions to be taken by the Council to comply the duty. The SoS Directions require the Council to, amongst others, continue to address the culture of poor financial management and to restore public trust and confidence by transforming the Council's activities, practices, and omissions to ensure that they are compatible with the best value duty. In addition, the Council is required to secure as soon as practicable that all its functions are exercised in conformity with the best value duty thereby delivering improvements in services and outcomes for the people of Croydon.

7.5 On 6 October 2023, The Improvement and Assurance Panel agreed an intervention Exit Strategy which describes the tangible improvements they expect the Council to make by March 2025. This includes in relation to Oracle IT system and how this operates in supporting the functions of the authority. Members will also be aware that reports have and are being taken to Mayor in Cabinet to seek approval for and provide updates on the Oracle Improvement Programme.

7.6 Comments approved by the Head of Litigation and Corporate Law on behalf of the Director of Legal Services and Monitoring Officer. (Date 08/03/24)

EQUALITIES IMPLICATIONS

7.7 The Council has a statutory duty to comply with the provisions set out in the Sec 149 Equality Act 2010. The Council must therefore have due regard to:

(a) eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act.
(b) advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it
(c) foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

7.8 In general, all IT systems should be monitored to ensure compliance with accessibility standards in relation to colleagues with disabilities, in particular relating to conditions related to some physical disabilities and neurodiverse conditions.

7.9 As this is an update report for noting, there are *no changes* to any systems or processes, therefore no direct impact on equalities identified.

7.10 Comments approved by: Helen Reeves, Head of Strategy & Policy, 06/03/2024.

8 APPENDICES

Appendix A. Presentation: Croydon Council Audit and Governance Committee – IT Controls 2022/23.

Appendix B: **Exempt**: IT Audit Findings 2022/23

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

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank