

Final Internal Audit Report

Application Audit: Housing Management systems

January 2025

Distribution: Interim Assistant Chief Executive
Director of Digital and Resident Access
Business Operations Manager
Interim Head of Specialist Systems
Information Security Manager
Corporate Director Resources (and S151 Officer)
Director of Finance and (and deputy S151 Officer)

Assurance Level	Issues Identified	
Limited Assurance	Priority 1	2
	Priority 2	2
	Priority 3	1

Confidentiality and Disclosure Clause

This report ("Report") was prepared by Forvis Mazars LLP at the request of London Borough of Croydon and terms for the preparation and scope of the Report have been agreed with them. The matters raised in this Report are only those which came to our attention during our internal audit work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, Internal Audit have only been able to base findings on the information and documentation provided and consequently no complete guarantee can be given that this Report is necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

The Report was prepared solely for the use and benefit of London Borough of Croydon and to the fullest extent permitted by law Forvis Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification. Accordingly, any reliance placed on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification by any third party is entirely at their own risk.

Please refer to the Statement of Responsibility in Appendix 3 of this report for further information about responsibilities, limitations, and confidentiality.

Contents
Page**Executive Summary**

1. Introduction	3
2. Key Issues	3

Detailed Report

3. Actions and Key Findings/Rationale	5
4. Priority 3 Findings	11

Appendices

1. Terms of Reference
2. Definitions for Audit Opinions and Identified Issues
3. Statement of Responsibility

1. Introduction

- 1.1 Croydon Council (Council) have been migrating its housing management system from Northgate Open Housing Management System to NEC Housing, which together with NEC Document Management, Net Call and CaseWorks comprise the key IT systems that support the housing service.
- 1.2 NEC Housing went live in June 2023, encompassing core processes and financials. In addition, it included integration with the NEC Revenues and Benefits system and interfaces with three contractors.
- 1.3 At the time of audit, phase 2 of the migration was underway, incorporating asset management, alongside task management and process automation, chain-based lettings, compliance management and rent arrears, amongst others.
- 1.4 As phase 2 was yet to be completed, the responsibility for application support and system administration had not yet transferred into the business applications support team from the project implementation team.
- 1.5 The responsibilities of managing the NEC application are split between the Council and NEC Software Solutions UK. Access to the application and the existing interfaces are all managed by the Council, while NEC Software Solutions UK manage application incidents, changes and resilience, with oversight from the Council.
- 1.6 This audit was undertaken as part of the agreed Internal Audit Plan for 2024/25 and assessed the key controls of both NEC Housing and NEC Document Management.

2. Key Issues

Priority 1 Issues

The Council had not conducted backup restoration tests of the NEC backups, and IT disaster recovery failover tests of the NEC application services. **(Issue 1)**

The final and approved copy of the contractual agreement between the Council and NEC Software Solutions UK was not provided for examination. **(Issue 4)**

Priority 2 Issues

There was a lack of adequate segregation of duties for privileged access to the NEC application and database. We observed two privileged users who had access to both the application and database. **(Issue 2)**

The monthly security reviews were not consistently conducted in accordance with established procedures. In addition, user access recertifications were not conducted by

Final Report

Digital Service Team (DST) in collaboration with the business process owners to verify whether access to various NEC roles by users is still required. **(Issue 3)**

The one 'Priority 3' issue is included under Section 4 below.

Draft for discussion purposes only

3. Actions and Key Findings/Rationale

Audit Area: Application Management and Governance

Priority	Action Proposed by Management	Detailed Finding/Rationale – Issue 1
1	<p>Update:</p> <p>Draft contract obtained from NEC along with copy of the signature page.</p> <p>Actions:</p> <p>Work with legal and procurement to find master version. (CDS Commercial Team)</p>	<p>Expected Control</p> <p>A contractual agreement that clearly defines the rights, responsibilities and obligations of the Council and NEC Software Solutions UK is documented and available for reference in the management of the supplier relationship.</p> <p>Finding/Issue</p> <p>Whilst phase 1 of NEC Housing went live in June 2023, the Council was unable to locate and provide evidence of the final and approved version of the NEC contractual agreement; therefore, examination of the agreement was unable to be completed to assess the design and implementation effectiveness of the vendor management and governance controls.</p> <p>Risk</p> <p>Without a contractual agreement at hand, it may be difficult for the Council to adequately monitor and determine the vendors non-compliance to among other things, data security, confidentiality, legal regulations and privacy requirements.</p>
<p>Responsible Officer</p> <p>Head of Specialist Systems</p>		
<p>Deadline</p> <p>End Jan 25</p>		

Audit Area: Access Management Controls

Priority	Action Proposed by Management	Detailed Finding/Rationale - Issue 2
2	<p>Update:</p> <p>There are two officers who need elevated access at certain times. We've reviewed our process around only providing the additional privileges when needed.</p> <p>There is a master access profile on the system which these roles do not have, and we would provide access for specific justified reasons.</p> <p>These role holders do not have the ability to create other admin accounts. Security and access controls are managed by the separate Digital Systems Team (DST).</p> <p>If the elevated access is needed, the officers need to request it via the DST who will activate the access needed.</p> <p>Actions:</p> <p>NEC Project Manager to confirm the process with DST Support Team Lead</p> <p>Publish this process and the joiners, movers and leavers process to the project team and Housing Digital Support Team (DST Support Team Lead).</p>	<p>Expected Control</p> <p>Privileged access refers to special access or abilities beyond those of a regular user. These elevated permissions allow users to perform critical system functions that are essential for the management, configuration, and security of IT systems. Privileged access to the database and application should be segregated to avoid conflicts of interest and reduce the risk of fraud.</p> <p>Finding/Issue</p> <p>Review of a system generated list of users with privileged access to the NEC application and database, found that there were two users with elevated access rights to both the application and database. The Housing Consultant explained that these are internal 'Housing System Implementation consultants'/application support and are not responsible for processing transactions. Their role is to provide technical support during the implementation of NEC.</p> <p>Risk</p> <p>A user with privileged access to both application and database can easily conduct system configuration changes, including user access rights, in the application and modify/ delete these changes in the database, thereby, going unnoticed.</p>
Responsible Officer		Deadline
Housing Support Team Manager		End Mar 25

Priority	Action Proposed by Management	Detailed Finding/Rationale - Issue 3
2	<p>Update:</p> <p>In many respects this is a symptom across all applications and not just NEC Housing and the ongoing issues with the joiners, leavers, and movers process.</p> <p><u>Joiners</u></p> <p>New user requests require a form to be completed by the line manager submitted to DST via the technical support portal. This needs to be reviewed so that security can be configured based on standard role profiles.</p> <p><u>Movers</u></p> <p>The current process requires line managers to inform CDS of changes in roles. There is no link from the HR system for CDS to be aware of changes although the HR workstream of the Oracle Fusion Improvement Programme is reviewing how this could be improved.</p> <p><u>Leavers</u></p> <p>CDS receives a monthly report on leavers from the HR system which is shared across DST. This report shows leavers to the establishment and does not include interims (something the HR workstream of the Oracle Fusion Improvement Programme is looking to address).</p> <p>On a monthly basis a security review is carried out to check financial limits against corporate organisational limits.</p> <p>Actions:</p>	<p>Expected Control</p> <p>Periodic user access reviews are performed to remove inappropriate access in a timely manner (for normal and privileged users). These verify that:</p> <ul style="list-style-type: none"> the user accounts are still valid (i.e., that the user is an active employee, contractor etc); access rights granted to the user account are aligned with the individuals' responsibilities within the organisation, including privileged access. <p>Finding/Issue</p> <p>The Digital Service Team (DST) management explained that monthly security reviews to identify and disable exited staff and inactive user accounts was conducted. However, on conducting an examination of the process, the following exceptions were found:</p> <ul style="list-style-type: none"> Security reviews were not conducted for two of the three sampled months; and User access recertifications were not conducted by DST in collaboration with the business process owners to verify whether access to various NEC roles by users was still appropriate. <p>Risk</p> <p>Without timely access review and removal of accounts associated with leavers, an employee may access gain unauthorised access to a leavers account, leading to inappropriate access to data and</p>

	<p>NEC Project to define the access roles on the system (NEC Project Manager).</p> <p>User Access form for new users, and changes to access, to be updated to reflect the agreed roles and the process validated so it complies with the Access Control Policy (see issue #5) (DST Support Team Lead).</p> <p>Communications exercise to confirm roles and responsibilities between service managers and DST (NEC Project Manager and DST Support Team Lead).</p> <p>Review joiners, movers and leavers process to ensure it is being followed consistently (DST Support Team Lead).</p> <p>We will update our process to log a ticket on Service Now to record when we conduct the security review and the outcomes from each one, aiming to conduct them monthly.</p>	<p>information. In addition, if a leaver is to rejoin the Council with a different role, they may retain access to sensitive data.</p> <p>Users may have access to inappropriate roles, which may lead to unauthorised access to data or information.</p>
Responsible Officer	Deadline	
NEC Project Lead	End March 25	

Audit Area: System Resilience and Recovery

Priority	Action Proposed by Management	Detailed Finding/Rationale - Issue 4
1	<p>Update:</p> <p>Being a hosted, SaaS platform we are constrained by the provision NEC have in the contract.</p> <p>NEC take a daily backup, and specific subsets of data have been restored from them.</p> <p>We have successfully cloned 'production' into other environments on a regular basis – this clone covers application configuration, user security and data.</p> <p>The NEC contract includes a failover provision, but this has not been tested. The NEC application and data are replicated across data centres so that in the event of an outage, the system can be switched over.</p> <p>To require a 'test' restoration or failover would be a chargeable piece of work – it wasn't included in the scope of the implementation project.</p> <p>Actions:</p> <p>Obtain quotes from NEC to undertake the test restoration and failover test (NEC Project Manager).</p> <p>Submit briefing note to the NEC Project Board outlining the cost to 'test' (NEC Project Manager).</p> <p>Decision on what actions to take (NEC Project Board – SRO: Corporate Director of Housing).</p>	<p>Expected Control</p> <p>Backups should be taken at least daily to an offsite location, and these backups should be subject to periodic restoration/ recovery testing based on pre-defined disaster scenarios and the test results clearly documented and communicated to management and those charged with governance to provide assurance that data can be recovered from these when required.</p> <p>Finding/Issue</p> <p>The NEC application is hosted in the primary datacentre (Hemel Hempstead 3), and the application servers are replicated to the secondary datacentre (NTT GDC), which serves as the disaster recovery site.</p> <p>The NEC Technical Design Architect explained that NEC Software Solutions conduct IT disaster recovery failover testing in response to client requests. These tests involve redirecting all the client's network traffic through a Virtual Private Network to NECs secondary datacentre. This provides clients with access to the secondary servers and databases for a specific period, allowing testing of services running in the disaster recovery datacentre.</p> <p>In addition, NEC Software Solutions can conduct backup restorations based on clients' requests and requirements, if requested. However, it was found that the Council had not conducted backup restoration testing of the NEC backups, and ITDR failover tests of the NEC application services.</p> <p>Risk</p>
Responsible Officer		Deadline

NEC Project Lead	End Feb 2025	<p>ITDR Failover tests verify that systems can be restored within the desired recovery time. Failing to conduct these tests may result in longer downtimes during an actual disaster, potentially impacting the Councils ability to meet its housing duties.</p> <p>Without periodic backup restoration tests, the Council may be unaware of any issues or errors in the backup process, such as corrupted files or incomplete back-ups, which could compromise data integrity and recovery efforts.</p>
------------------	--------------	--

4. Priority 3 Findings

Audit Area: Application Management and Governance

Agreed action	Findings
<p><u>Action proposed by management:</u></p> <p>Update:</p> <p>Whilst NEC Housing has been in 'project mode' it has maintained internal documentation relating to changes.</p> <p>Going forward it will adopt the formal ITIL Change process as defined by CDS as required of other applications which includes a Change Advisory Board (CAB). The current change process is being reviewed within CDS to improve several areas including adopting a more consistent approach for SaaS applications across the estate. NEC Housing will benefit from these improvements once agreed and implemented.</p> <p>The CDS Cyber Security Manager has been progressing the approval of several security policies, including the Access Control Policy. All such policies are covered by a separate audit (reference here) are being reviewed and should be formally signed off in the near future.</p> <p>Actions:</p> <p>CDS to confirm current Change Management process and to work with NEC project team to ensure</p>	<p>Expected Control</p> <p>Information Technology policies and procedures are defined, documented, and communicated with key personnel.</p> <p>Finding/Issue</p> <p>While the Council had defined application change and user access control processes, the below exceptions were identified:</p> <ul style="list-style-type: none">• A change control policy had not been established and documented; and• The "Access Control Policy" document was still in draft and had not been approved by management. <p>Risk</p> <p>Lack of a change control policy may lead to inconsistencies and non-compliance to established change management process.</p> <p>Without management authorisation of the "Access Control Policy" document, employees may not feel obligated to comply to the policy/procedure manual.</p>

Agreed action	Findings
<p>future changes follow this process (CDS DST Squad Manager).</p> <p>Formal management sign-off of Access Control Policy dependant on another Mazars audit (CDS Cyber Security Manager).</p> <p>Once Access Control Policy has been signed off, review all access control procedures to ensure it is being complied with (DST Support Team Lead).</p> <p>Responsible Officer: Head of Specialist Systems</p> <p>Deadline: End April 2025</p>	

AUDIT TERMS OF REFERENCE

Application Audit: Housing Management systems

1. INTRODUCTION

- 1.1 The Council recently migrated its housing management system from Northgate Open Housing Management System to NEC Housing, which together with NEC Document Management, Net Call and CaseWorks comprise the key IT systems that support the housing service.
- 1.2 NEC Housing went live in June 2023, encompassing core processes and financials. In addition, it included integration with NEC Revenues and Benefits system, and interfaces with three contractors.
- 1.3 Currently, phase 2 is underway, incorporating asset management, alongside task management and process automation, chain-based lettings, compliance management and rent arrears, amongst others.
- 1.4 As Phase 2 has yet to be completed, the responsibility for application support and system administration has yet to transfer into the business applications support team from the project implementation team.
- 1.5 This audit is being undertaken as part of the agreed Internal Audit Plan for 2024/25 and will assess the key controls of NEC Housing.

2. OBJECTIVES AND METHOD

- 2.1 The overall audit objective is to provide an objective independent opinion on the adequacy and effectiveness of controls / processes.
- 2.2 The audit will for each controls / process being considered:
 - Walkthrough the processes to consider the key controls
 - Conduct sample testing of the identified key controls, and
 - Report on these accordingly.

3. SCOPE





- 2.3 This audit, which focused on management of the NEC application, was undertaken as part of the 2024/25 Internal Audit Plan. The specific scope included the following areas and recommendations:

Audit Area	Identified Issues		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Application Management and Governance	1	0	1
Access Management Controls	0	2	0
Data Integrity – Data input and interfaces	0	0	0
System Resilience and Recovery	1	0	0
Totals	2	2	1

Definitions for Audit Opinions and Identified Issues

In order to assist management in using our reports:

We categorise our **audit assurance opinion** according to our overall assessment of the risk management system, effectiveness of the controls in place and the level of compliance with these controls and the action being taken to remedy significant findings or weaknesses.

	Full Assurance	There is a sound system of control designed to achieve the system objectives, and the controls are constantly applied.
	Substantial Assurance	While there is basically a sound system of control to achieve the system objectives, there are weaknesses in the design or level of non-compliance of the controls which may put this achievement at risk.
	Limited Assurance	There are significant weaknesses in key areas of system controls and non-compliance that puts achieving the system objectives at risk.
	No Assurance	Controls are non-existent or extremely weak, leaving the system open to the high risk of error, abuse, and reputational damage.

Priorities assigned to identified issues are based on the following criteria:

Priority 1 (High)	Fundamental control weaknesses that require immediate attention by management to action and mitigate significant exposure to risk.
Priority 2 (Medium)	Control weakness that still represent an exposure to risk and need to be addressed within a reasonable period.
Priority 3 (Low)	Although control weaknesses are considered to be relatively minor and low risk, still provides an opportunity for improvement. May also apply to areas considered to be of best practice that can improve for example the value for money of the review area.

Statement of Responsibility

We take responsibility to the London Borough of Croydon for this report which is prepared on the basis of the limitations set out below.

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.

This report is confidential and must not be disclosed to any third party or reproduced in whole or in part without our prior written consent. To the fullest extent permitted by law Forvis Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation amendment and/or modification by any third party is entirely at their own risk.

Registered office: 30 Old Bailey, London, EC4M 7AU, United Kingdom. Registered in England and Wales No 0C308299.