

Final Internal Audit Report

Northgate iWorld Application

December 2019

Distribution: Executive Director of Resources and Monitoring Officer (Final only)
Chief Digital Officer
Business Manager
Support Services Manager
Technical Support and Development (TSD) Manager.

Assurance Level	Identified Issues	
Substantial	Priority 1	-
	Priority 2	1
	Priority 3	-

Confidentiality and Disclosure Clause

This report ("Report") was prepared by 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 has 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 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, re-interpretation, amendment and/or modification. Accordingly, any reliance placed on the Report, its contents, conclusions, any extract, re-interpretation, 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.....	4

Detailed Report

3. Actions and Key Findings/Rationale.....	5
--	---

Appendices

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

1. Introduction

- 1.1 London Borough of Croydon (LBC) has been in contract with Northgate Public Services (NPS) to supply cloud-based software for the management and processing of its revenue and benefits activities, for at least the last ten years. The contract was last extended/renewed during 2015. The software is hosted by NPS as Software as a Service, reducing the administration required by LBC, without transferring responsibility for the provision of the application for business users, and for the associated data. Roles and responsibilities of NPS and the Council have been agreed and set out in the software contract.
- 1.2 The Northgate iWorld application software licenses are managed and controlled via an online portal provided by Northgate Public Services (NPS), which is reviewed and updated where necessary and stores up to date user guides, release notes and any other relevant information for customers. The system has not been customised so the guidance remains relevant on an annual basis to ensure that all staff groups and relevant modules are properly licensed.
- 1.3 The Northgate system software as a service agreement provides the following services:
 - Communications;
 - Monitoring;
 - Back-up;
 - Operating system;
 - Hardware maintenance;
 - Application management;
 - Database administration;
 - Support and maintenance.
- 1.4 BACS submission files for council tax, housing benefits and business rates refunds processed are reconciled to Northgate, then approved by a delegated officer and provided to Finance for upload to Oracle. Routine monitoring of the success of back-ups is undertaken each day by NPS, with a weekly report provided to LBC as confirmation.
- 1.5 System password settings have been set in accordance with the Information Security Management System (ISMS). The ISMS is the Council's Information Security Policy which is split into part 1 – standard users and part 2 – IT staff. The Technical Support and Development (TSD) team monitors, reviews and investigates failed system access attempts and maximum log in attempts reached on a monthly basis. Adequate separation of duties has been configured through the system settings for each job role at officer and supervisor/manager level. A review of system job roles noted that separation of duties has been built into access permissions, for example processing and approving refunds.
- 1.6 Northgate system release notes and release schedules are provided by Northgate prior to any changes being implemented, which are reviewed by TSD and formulated into a test plan. Test results are recorded and reviewed prior to sign off of acceptance. Quarterly performance meetings take place between LBC and NPS, where service performance reports are provided, discussed, and any actions identified are agreed and reported back at the next meeting.
- 1.7 Disaster recovery arrangements are in place and are tested on an annual basis. However, disaster recovery testing did not formally happen in 2019 due to a data centre move. This in essence was completed as a real disaster recovery scenario in that during October 2019 a copy of the live environment was deployed at a new data centre.

2. **Key Issue**

Priority 2 Issue

The process for assigning modules/roles for new users set up on the system was flawed and there was no established process for managers to notify and provide approval to when users require additional or reduced access (**Issue 1**).

There were no priority 3 issues identified.

3. Actions and Key Findings/Rationale

Control Area 01: Application management and governance						
Priority	Action Proposed by Management	Detailed Finding/Rationale – Issue 1				
2	<p>The following actions have been agreed and are either complete or in progress.</p> <ul style="list-style-type: none"> ○ Current form to be updated to add specific job roles – by 13th Dec ○ Add change of responsibilities to form - by 13th Dec ○ Provide documentation re job roles and guidance for access – 31st Dec ○ Add audit process – review of non-access and removal of access (disable account) after 90 days non use – 31st Jan 	<p>Business managers are responsible for requesting and approving new users for access to be granted to Northgate, by completing, approving and emailing a new starter form to TSD. TSD then creates the new user based on the information provided.</p> <p>The following was identified:</p> <ol style="list-style-type: none"> 1. The new starter form does not require managers to specify which modules/roles a user should be granted access to, but provides the user ID of a colleague which is used to clone the new user’s access permissions granted; the TSD team are required to use their best judgement when granting access, based on the user’s job role, team and cloned user details; 2. There is no documentation providing details of the definition of system job roles, and new TSD staff are unaware of what access the job roles include to ensure that users do not have access to potentially sensitive data they do not have a business need for; 3. There is no established process for managers to notify and provide approval to TSD when users require additional or reduced access, and additional job roles cannot be time limited, for example where additional access is required on a temporary basis; <p>A sample of user forms for 7 new users was tested and the following was noted:</p> <ul style="list-style-type: none"> • 5 users had been granted the same access role profile as the cloned user; • A user had been granted access to more roles than their cloned user; • A user had been granted access to less roles than their cloned user. 				
	<table border="1"> <thead> <tr> <th>Responsible officer</th> <th>Deadline</th> </tr> </thead> <tbody> <tr> <td>Support Services Manager</td> <td>31st January 2019</td> </tr> </tbody> </table>	Responsible officer	Deadline	Support Services Manager	31 st January 2019	<p>There is therefore no assurance that users of Northgate have been granted and maintain the correct access rights to the system and its modules, based on system job role requirements and service area responsibilities. This could result in users having access to potentially sensitive data which they have no business need for.</p>
Responsible officer	Deadline					
Support Services Manager	31 st January 2019					

TERMS OF REFERENCE

1. INTRODUCTION AND BACKGROUND

- 1.1 The Northgate iWorld application is a key line of business and is used by and for the administration of Council Tax, Housing Benefit, Council Tax Support and Business Rates. It is supplied by Northgate (NPS) and the main users of the system are:
- Council Tax (Revenues Team)
 - Housing Benefits Team
 - Corporate Debt Team
 - Enforcement Team
 - Gateway Teams
- 1.2 The Northgate iWorld application audit will be performed to ensure that controls have been adequately designed and implemented to ensure effective IT security, linkages/interfaces with other council infrastructures and systems.
- 1.3 This audit is part of the Internal Audit Plan for 2019/20 as agreed by the General Purposes and Audit Committee.

2. OBJECTIVES AND METHODOLOGY

- 2.1 The overall audit objective of this audit is to provide an objective independent opinion on the adequacy and effectiveness of the control environment with regards to the Northgate iWorld application.
- 2.2 In order to achieve the overall objectives, a risk based systems audit approach will be carried out, documenting and evaluating the actual controls against those expected and based on this, undertaking appropriate audit testing.
- 2.3 The key findings, conclusions, and subsequent recommendations arising will be discussed with management at an exit meeting, followed by the circulation of a draft report for consideration, prior to agreement and issue of the final audit report.

3. SCOPE





- 3.1 This audit examined the following areas:

Control Areas/Risks	Issues Identified		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Application management and governance	0	1	0
System security	0	0	0
Interface controls and data processing	0	0	0
Change control	0	0	0
System resilience and recovery	0	0	0
Support arrangements	0	0	0
TOTAL	0	1	0

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 consistently 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 which may put this achievement at risk.
	Limited Assurance	There are significant weaknesses in key areas of system controls and/or non-compliance that puts achieving the system objectives at risk.
	No Assurance	Controls are non-existent or weak and/or there are high levels of non-compliance, leaving the system open to the high risk of error or abuse which could result in financial loss and/or reputational damage.

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

Priority 1 (High)	Fundamental control weaknesses that require the immediate attention of management to mitigate significant exposure to risk.
Priority 2 (Medium)	Control weakness that represents an exposure to risk and requires timely action.
Priority 3 (Low)	Although control weaknesses are considered to be relatively minor and low risk, action to address still provides an opportunity for improvement. May also apply to areas considered to be of best practice.

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, 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: Tower Bridge House, St Katharine's Way, London E1W 1DD, United Kingdom.
Registered in England and Wales No 0C308299.