

NCH Use of Lagan Frontline (Contact Centre IT System) Final Audit Report

Contents of Report		Page
1	Introduction & Background	2
2	Audit Approach	2
3	Objective	3
4	Main Conclusions	3
5	Findings in Detail	4

Document title:	nchlaganfinalrep.doc
Issue Date:	22 February 2008
Issued to:	Julie Crook, Director of Finance & ICT, NCH
Copied to:	Paul Martin, Head of ICT, NCC

Contact Details:		
Head of Risk and Audit Services	Shail Shah	X54050
Audit Manager	Adrian Whiteley	X54822
Auditor	Ranjit Sahota	X54039

1 Introduction & Background

- 1.1 The Audit Commission concluded in its “Access to Service” report dated May 2005, that Council service provision was ‘fair with promising prospects for improvement’.
- 1.2 In order to improve service provision, the City Council made a commitment to establish a corporate contact centre as part of the Customer Service Transformation strategy which gained approval by the Councils Executive board in September 2005.
- 1.3 A key component of the strategy is a new Customer Relationship Management (CRM) software application, which was purchased and deployed to handle all ‘first point of contact’ queries raised by residents of Nottingham.
- 1.4 Lagan Frontline is the Council’s CRM solution. The product is Java based with an SQL 2005 backend database operating on a Windows 2003 Server platform
- 1.5 The audit was commissioned as part of the 2007/08 programme of agreed IT-related audits, carried out for Nottingham City Homes by Nottingham City Council.

2 Audit Approach

- 2.1 An Audit was undertaken of the Lagan Frontline software implementation to ensure that effective controls had been incorporated into the overall design and operational aspects of the software implementation.
- 2.2 The main focus of the audit was to provide assurance to Nottingham City Homes (NCH) that the software deployment provided adequate privacy of data and protection from unauthorised access.
- 2.3 In order to provide assurance Internal Audit examined, the following areas:-
 - Access controls especially User Management procedures
 - Effectiveness of Audit trails
 - Backup and Recovery procedures including business continuity
- 2.4 The Audit was conducted by way of discussions with staff from:
 - Customer Contact Centre project team,
 - ICT (Resources)
 - ICT (NCH)
 - NCH
- 2.5 In addition pertinent documentation such as System Documentation, User / Operations manuals were examined and testing undertaken specifically for NCH User management procedures.

3 Objective

- 3.1 The Object of this review is to provide assurance to the Responsible Head in Nottingham City Homes on the effectiveness of controls over the implementation and operation of the Lagan Frontline Software.

4 Main Conclusions

- 4.1 At the time of the review the software was relatively newly-implemented, having been operational for about nine months.
- 4.2 The call centre project has not been fully signed off yet, and it is understood that an audit at this stage would find some deficiencies. Therefore although this report can only give limited assurance on the effectiveness of IT security controls, it is understood that the team responsible for the project have every intention of making progress in these areas:
- Strengthening of user management and password controls
 - Improvements to documentation
 - Improving service level agreements so that continuity of system availability, and support arrangements, is better assured.
- 4.3 These improvements are required both to comply with internal security policies and to comply with statutory obligations under the Data Protection Act 1998.
- 4.4 From the perspective of NCH pursuing the recommendations in this report, the key factor is for the Central Rents Team Manager and the Head of IT NCH to agree service levels and action plans with the City Council service provider.

5 Findings in Detail

User Management

- 5.1 Effective User Management procedures are considered to be an essential component of any IT security framework and a good method of being able to demonstrate compliance with relevant Acts of Parliament such as the Data Protection Act 1998.
- 5.2 During the course of this audit a review of User Management procedures was undertaken to ensure that all NCH users setup on the system were authorised and certified to use the system. A total of 24 users were extracted from the SQL 2005 database and reconciled with documentation (user setup requests, emails) supplied to us by the business process re-engineering team leader. We were unable to find appropriate authorisation for a number of Users; however, upon further investigation we were notified that some users were setup as a 'bulk' exercise. We were unable to verify this from the documentation supplied.
- 5.3 A review of the documentation revealed that there was inadequate segregation of duties for setting up users. From the 7 User Setup / Deletion forms supplied, 2 were signed and authorised by the System Administrator and 1 had been authorised by the System Administrator. At the time of the review, City Audit Services were informed that the User Management function was in the process of being transferred to the IT Help Desk.

Recommendation

- R1. *In order to enforce segregation of duties the transfer of User Management to the IT Helpdesk is recommended. However, authorisation and certification of access should remain the responsibility of the relevant NCH service manager and authorisation compliance reviews need to be an integral part of the process*
- 5.4 A detailed examination was undertaken of the 24 user details extracted mentioned in 5.2, to ensure that they were current and active. City Audit Services found 4 dormant accounts and only one of these had been locked. Dormant accounts are a high risk because they are easy for an intruder to break into.
- 5.5 Access to the software application is controlled via the allocation of a unique User-id and associated password. The password strength (4 Characters) is weak and does not comply with the corporate IT security policy (6 Characters); furthermore, out of the 24 user accounts reviewed 14 contained a 'Null' value in the password expiry field, which is contrary to the Policy requirement that passwords are regularly changed.

Recommendations

- R2. *User Accounts should be reviewed on regular basis to ensure that dormant accounts are removed or locked from the system*

- R3 *Password Management should be reviewed to ensure that they comply with the corporate IT security policy.*

Audit Trails

- 5.6 Lagan Frontline provides a wealth of auditing data that is built into the system. However, the type, extent and level of auditing has yet to be defined, documented and agreed with relevant stakeholders in order for it to be configured, implemented and managed. There are two types of log in Frontline, Client and Server. Client logs are specific to activities carried out on each Frontline client. These logs are usually stored on the C drive of the client machine and not subject to any routine backup. Server logs record activities specific to each service. At the time of the audit the log level setting was set at 9, which outputs the lowest level of detail, however, log level 1 provides the most detail, but would critically impact on the performance of the software and its use should be limited. At the time of the review, City Audit Services were notified by the project officer that the auditing process had not been ratified

Recommendations

- R4 *The extent, type and level of auditing, should to be established, proportionate to the risks being addressed. Incident Management procedures should to be set up to deal with the analysis, reporting and handling of audit events that are considered to be a risk.*
- R5 *Client audit logs should be subject to normal backup and restoration process*

Backup & Recovery (Business Continuity)

- 5.7 City Audit services were unable to find any formal documented business continuity plans. Such documentation would incorporate risk assessment and business impact analysis plans, in order to effectively manage prolonged unavailability of Lagan Frontline Software.
- 5.8 There was no Service Level agreement in place between NCH and the City Council IT Department, specifically, for the provision and use of the Lagan Frontline software product. Such agreement would incorporate Backup / Recovery and business continuity arrangements.

Recommendation

- R6 *Service Level agreements should be established defining the required service levels for backup and recovery, and referring to business continuity plans to manage incidents of prolonged unavailability of IT resources.*
- 5.9 A technical evaluation of IT Security risks was not incorporated into the implementation project plan. Such an evaluation would provide assurance that the IT architecture on which Frontline operates and places reliance is securely configured. In the absence of such an evaluation, it is not possible to provide assurance that the software is operating in a secure environment and furthermore that all risks are identified, understood and evaluated.

Recommendation

R7 A technical security evaluation of the ICT infrastructure should be undertaken to ensure that Lagan Frontline is operating in an appropriately secure environment.

- 5.10 During the course of the review we were unable to obtain ready access to pertinent system administration documentation. This could be due to the fact that system administration duties are performed by different people; for example, End Users, ICT Projects and ICT Infrastructure. City Audit services also found that documentation produced as part of the project held within the ICT Infrastructure was not being kept up to date to reflect changes in working practices and furthermore were incomplete (backup restoration process), this shortcoming was recognised by the technical analyst within the ICT Infrastructure section.
- 5.11 Lagan Frontline software runs on the Windows 2003 server operating system platform; however, it is important to ensure that individuals tasked with supporting this environment have undertaken accredited training in order demonstrate their competence and provide a level of assurance that they are able to effectively support the environment. Discussions held with the two Technical Analysts, who support the platform has revealed that they have not undertaken any accredited training in Windows 2003 server platform.

Recommendation

R8 Staff undertaking support functions should be trained in the technical platforms that they support, furthermore, a mechanism should be in place to ensure that system documentation is kept up to date and reflects current working practices.

6 Action Plan

Ref	Recommendation	Priority	Management Response	Responsibility and Target Date
R1	In order to enforce segregation of duties the transfer of User Management to the IT Helpdesk is recommended. However, authorisation and certification of access should remain the responsibility of the relevant NCH service manager and authorisation compliance reviews need to be an integral part of the process	H	Will agree effective process with NCC	Central Rents Team Manager and the Head of IT (NCH) June 2008
R2	User Accounts should be reviewed on regular basis to ensure that dormant accounts are removed or locked from the system	H	Will work through list of accounts with NCC to remove inappropriate accounts.	Central Rents Team Manager and the Head of IT (NCH) April 2008
R3	Password Management should be reviewed to ensure that they comply with the corporate IT security policy.	M	Will obtain options of improving password controls from NCC	Central Rents Team Manager and the Head of IT (NCH) June 2008
R4	The extent, type and level of auditing, should to be established, proportionate to the risks being addressed. Incident Management procedures should to be set up to deal with the analysis, reporting and handling of audit events that are considered to be a risk.	M	Will agree effective process with NCC	Central Rents Team Manager and the Head of IT (NCH) June 2008
R5	Client audit logs should be subject to normal backup and restoration process	H	Will agree effective process with NCC	Head of IT (NCH) June 2008

Ref	Recommendation	Priority	Management Response	Responsibility and Target Date
R6	Service Level agreements should be established defining the required service levels for backup and recovery, and referring to business continuity plans to manage incidents of prolonged unavailability of IT resources.	M	Will establish SLA's and define service level required for backup, restore, and disaster recovery.	Central Rents Team Manager and the Head of IT (NCH) July 2008
R7	A technical security evaluation of the ICT infrastructure should be undertaken to ensure that Lagan Frontline is operating in an appropriately secure environment.	M	Will obtain assurances from NCC that this is part of the project.	Head of IT (NCH) April 2008
R8	Staff undertaking support functions should be trained in the technical platforms that they support, furthermore, a mechanism should be in place to ensure that system documentation is kept up to date and reflects current working practices.	M	Will include support staff capability as part of SLA	Head of IT (NCH) July 2008

Signed..... Date.....
(3rd tier manager or above)

Glossary of Terms

1 Categorisation of Recommendations

The recommendations within this report have been categorised by City Audit Services as:

High Priority	A fundamental weakness which presents material risk to the audited body and requires urgent attention by management.
Medium Priority	A significant weakness whose impact or frequency presents an unacceptable risk to the audited body that should be addressed by management.
Low Priority	The audited body is not exposed to any significant risk, but the recommendation merits attention.

In all cases Internal Audit will follow up implementation of the recommendations by the agreed date.