



NOTTINGHAM CITY HOMES

REVIEW OF THE IT SECURITY - NETWORK CONTROLS ARRANGEMENTS

Report issued:	August 2009
-----------------------	-------------

Audit Plan:	2009/10
--------------------	---------

The matters raised in this report are only those that came to the attention of the auditor during the course of the internal audit review and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that might be made. This report has been prepared solely for management's use and must not be recited or referred to in whole or in part to third parties without our prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other purpose. TIAA neither owes nor accepts any duty of care to any other party who may receive this report and specifically disclaims any liability for loss, damage or expense of whatsoever nature, which is caused by their reliance on our report.

Business Assurance

Review of the IT Security – Network Controls Arrangements

- EXECUTIVE SUMMARY -

INTRODUCTION

1. We have reviewed the IT Security – Network Controls arrangements at Nottingham City Homes (NCH). The review was carried out in June 2009 as part of the planned internal audit work for 2009/10.

SUMMARY

2. Two Key Risk Control Objectives were identified and tested and based on the findings from this work an overall evaluation of the overall adequacy of the internal controls was established. (figure 1 below).

Figure 1 - Evaluations of the Effectiveness of the Internal Controls

Evaluation
<u>Limited Assurance</u>

KEY FINDINGS

3. The key control and operational practice findings that need to be addressed in order to strengthen the control environment are set out in the Management and Operational Effectiveness Action Plans. The prioritisation of the findings are summarised below (figure 2):

Figure 2 - Summary of Priorities of Findings

Urgent	Priority	Routine	Operational
	7	3	

MANAGEMENT RESPONSES

4. Recommendations for improvements should be assessed by NCH for their full impact before they are implemented.

RELEASE OF REPORT

5. The table below sets out the history of this report.

Date draft report issued:	10 th June 2009
Date management responses recd:	10 th August 2009
Date final report issued:	12 th August 2009



MANAGEMENT ACTION PLAN
PRIORITY 1, 2 AND 3 RECOMMENDATIONS

Risk	Finding	Recommendation	Priority	Management Comments	Implementation Timetable	Responsible Officer
Failure to direct the process through approved policy & procedures.	Whilst a more up to date Nottingham City Council (NCC) set of Security and Acceptable Use policies have been released these could be seen as confusing for staff as many supporting documents are not available with other processes not being applicable to NCH staff. This greatly increases the risk of security breaches.	Recommendation 1: NCH be required to develop its own set of Security and Acceptable Use policies which reflect the needs and the processes of NCH.	2	Full set of NCH's own ICT policies and procedures is planned. Work to commence once key service SLAs have been negotiated (due to interdependence).	End September 2009	Robert Allen – Head of ICT

PRIORITY GRADINGS

1	URGENT	fundamental control issue on which action should be taken immediately.
---	--------	--

2	IMPORTANT	control issue on which action should be taken at the earliest opportunity.
---	-----------	--

3	ROUTINE	control issue on which action should be taken.
---	---------	--



Risk	Finding	Recommendation	Priority	Management Comments	Implementation Timetable	Responsible Officer
Failure to direct the process through approved policy & procedures.	At present, NCH staff are not required to periodically 'sign up' to having read and understood Security and acceptable use policies. This places the Company at risk in that staff may not understand and not follow security/data protection measures leading to non accountability should a deliberate or inadvertent security breach occur.	Recommendation 2: All staff be required to sign to confirm that they have read and understand the relevant IT Security Policies.	2	<i>Will require signature of staff against new policies once in place.</i>	<i>End of October 2009</i>	<i>Robert Allen – Head of ICT</i> <i>Supported by ICT team HR officer.</i>

PRIORITY GRADINGS

1	URGENT	fundamental control issue on which action should be taken immediately.
---	--------	--

2	IMPORTANT	control issue on which action should be taken at the earliest opportunity.
---	-----------	--

3	ROUTINE	control issue on which action should be taken.
---	---------	--



Risk	Finding	Recommendation	Priority	Management Comments	Implementation Timetable	Responsible Officer
Failure to direct the process through approved policy & procedures.	It was ascertained that not all the day-to-day processes and procedures are fully documented. This means there is a risk that should key staff leave or be absent for a considerable period of time there could be incorrect action and decisions taken by the team.	Recommendation 3: The IT Support team be required to review its documentation to ensure that all key processes and procedures are documented, version controlled and dated.	2	<i>Work already in progress. ICT team will be working with Business Improvement Team to review version control etc.</i>	<i>Ongoing (new systems and changes frequently occur)</i>	Robert Allen – Head of ICT
		Recommendation 4: The IT Support team be required review and update all procedural documentation following the implementation of new systems, system upgrades and changes in processes.	3	<i>As above.</i>		

PRIORITY GRADINGS

1	URGENT	fundamental control issue on which action should be taken immediately.
---	--------	--

2	IMPORTANT	control issue on which action should be taken at the earliest opportunity.
---	-----------	--

3	ROUTINE	control issue on which action should be taken.
---	---------	--



Risk	Finding	Recommendation	Priority	Management Comments	Implementation Timetable	Responsible Officer
Unauthorised access to the network, affecting the availability, integrity and/or confidentiality of data.	NCH do not periodically receive logs of user activity for Network, Internet or email usage resulting in the primary method of identifying suspicious activity rests with NCC who do not necessarily know how to interpret NCH business needs.	Recommendation 5: NCH obtain monthly logs of User activity in the areas of Network, Internet and email usage and carry out a series of checks looking for actual or attempted misuse/abuse.	3	<i>Discussions are in progress with NCC Networks and Security Manager to arrange for proper reporting on such issues.</i>	<i>End of September 2009</i>	<i>Robert Allen – Head of ICT</i>
Unauthorised access to the network, affecting the availability, integrity and/or confidentiality of data.	NCH does not possess its own Security Incident Management process but again relies on NCC to deal with this (indeed the Security policy as referred to above points NCH staff at NCC). This places NCH at risk of incorrect management of any incidents as business knowledge is unlikely to be correctly utilised.	Recommendation 6: NCH establishes its own Security Incident Management process and ensured that all suspected incidents are first notified to the relevant NCH personnel.	3	<i>SIM process is to be fully considered during current SLA negotiations.</i>	<i>End of December 2009</i>	<i>Robert Allen – Head of ICT</i>

PRIORITY GRADINGS

1	URGENT	fundamental control issue on which action should be taken immediately.
---	--------	--

2	IMPORTANT	control issue on which action should be taken at the earliest opportunity.
---	-----------	--

3	ROUTINE	control issue on which action should be taken.
---	---------	--



Risk	Finding	Recommendation	Priority	Management Comments	Implementation Timetable	Responsible Officer
Unauthorised access to the network, affecting the availability, integrity and/or confidentiality of data.	There are three members of the IT Team with partial administrator Network access but their rights and abilities are not documented and indeed are not known in full detail. This places NCH at risk of incorrect or inefficient action being taken by those staff	Recommendation 7: The exact details of the partial administrator access rights granted to NCH staff be documented and held by both NCH and NCC.	2	<i>Administrative privileges to be closely restricted to ICT staff and documented.</i>	<i>End of December 2009</i>	<i>Robert Allen – Head of ICT</i>

PRIORITY GRADINGS

1	URGENT	fundamental control issue on which action should be taken immediately.
---	--------	--

2	IMPORTANT	control issue on which action should be taken at the earliest opportunity.
---	-----------	--

3	ROUTINE	control issue on which action should be taken.
---	---------	--



Risk	Finding	Recommendation	Priority	Management Comments	Implementation Timetable	Responsible Officer
Unauthorised access to the network, affecting the availability, integrity and/or confidentiality of data.	There is no formal process of reviewing whether or not all User access rights granted are still necessary (although the IT Team do their best to review users they do not have detailed knowledge of the individual roles). There is therefore a risk that users retain access to systems and data that they have no authorised business need to access.	Recommendation 8: All Managers be required to carry out a review of all their staff system access requirements for their current role. This review be carried out on an annual basis (or more frequent if NCH deem necessary).	2	<i>To be implemented for Northgate housing management system, ROCC and OneWorld as the Company's key systems.</i> <i>Subsequent reviews will be bi-annually.</i>	<i>End of December 2009</i>	<i>Application Support and Development Team Manager</i>

PRIORITY GRADINGS

1	URGENT	fundamental control issue on which action should be taken immediately.
---	--------	--

2	IMPORTANT	control issue on which action should be taken at the earliest opportunity.
---	-----------	--

3	ROUTINE	control issue on which action should be taken.
---	---------	--



Risk	Finding	Recommendation	Priority	Management Comments	Implementation Timetable	Responsible Officer
The network is disrupted, or data is lost, due to the failure or network devices and inadequate recovery procedures.	NCH have not advised NCC of their prioritised requirements for the restoration of computer systems in the event of a disaster occurring. Currently, only the housing management system will be restored urgently and all other systems may take weeks to restore thus placing NCH at risk of serious business disruption.	Recommendation 9: NCH completes its Business Continuity Plan (which includes Disaster Recovery arrangements) as soon as possible and negotiates appropriate timescales for restoration of services by NCC. In addition NCH should ensure that it is involved in the Disaster Recovery testing programme on a periodic basis.	2	Completion of the NCH Business Continuity Plan is included in the Health and Safety Strategy. ICT business continuity and disaster recovery arrangements to be included in SLA negotiations for each individual service.	End of July 2010 End of December 2009	Ian Rabett – Head of Health and Safety Robert Allen – Head of ICT

PRIORITY GRADINGS

1	URGENT	fundamental control issue on which action should be taken immediately.
---	--------	--

2	IMPORTANT	control issue on which action should be taken at the earliest opportunity.
---	-----------	--

3	ROUTINE	control issue on which action should be taken.
---	---------	--



Risk	Finding	Recommendation	Priority	Management Comments	Implementation Timetable	Responsible Officer
Networks are properly managed, with controls existing over error reporting and clearance, external connections and internet/email access.	The change control process operated in conjunction with NCC is currently not operating correctly meaning that any appropriate impact on any changes made to network or systems may not be known or identified.	Recommendation 10: NCH be required to ensure that the change control process is operated correctly and effectively.	2	<i>Data Networks SLA will have availability and Change Control aspects agreed and formalised with NCC.</i>	<i>End of Dec 2009</i>	<i>Robert Allen – Head of ICT</i>

PRIORITY GRADINGS

1	URGENT	fundamental control issue on which action should be taken immediately.
---	--------	--

2	IMPORTANT	control issue on which action should be taken at the earliest opportunity.
---	-----------	--

3	ROUTINE	control issue on which action should be taken.
---	---------	--

- DETAILED REPORT -

SCOPE AND LIMITATIONS OF THE REVIEW

6. The review considered the arrangements for the physical and access security of hardware and software. The scope of the review does not include consideration of the merits of the types of hardware and software used, the access rights to the individual software; or the depreciation policies.
7. The limitations and the responsibilities of management in regard to this review are set out in the Annual Plan.

ASSESSMENTS OF THE KEY RISK CONTROL OBJECTIVES

8. This review identified and tested the controls that are being operated by NCH and an assessment of the combined effectiveness of the controls in mitigating the key control risks is provided. The assessments are:

Substantial Assurance	robust series of internal controls in place which should ensure continuous and effective achievement of the control objective.
Reasonable Assurance	reasonable number of internal controls in place, however may not be operated all the time.
Limited Assurance	the controls in place are not sufficient to ensure the continuous and effective achievement of the control objective.
No Assurance	fundamental breakdown or absence of core internal controls.

MATERIALITY

9. NCH is dependent on its IT Network Systems to deliver day-to-day operation of the Company. It is essential for normal working that internal and remote network access is maintained at a maximum level and that the service is provided with adequate confidentiality, integrity and availability.

AUDIT FINDINGS

10. Risk	Failure to direct the process through approved policy & procedures
Risk Control Objective	Arrangements in place provide for compliance with established policies, procedures, laws and regulations
Evaluation	<u>Limited</u>

11 The following matters were identified in reviewing the Key Risk Control Objective:

11.1 The majority of Nottingham City Homes' (NCH) IT provision is by means of a contract with Nottingham City Council (NCC) IT Department. At the time of this review the Management Responses had not been given to a report issued in February 2009 although responses have now been made and the February report finalised.

11.2 Whilst a more up to date Nottingham City Council (NCC) set of Security and Acceptable Use policies have been released these could be seen as confusing for staff as many supporting documents are not available with other processes not being applicable to NCH staff. This greatly increases the risk of security breaches.

Recommendation 1: NCH be required to should develop its own set of Security and Acceptable Use policies which reflect the needs and the processes of NCH.

11.3 At present, NCH staff are not required to periodically 'sign up' to having read and understood Security and acceptable use policies. This places the Company at risk in that staff may not understand and not follow security/data protection measures leading to non accountability should a deliberate or inadvertent security breach occur.

Recommendation 2: All staff be required to sign to confirm that they have read and understand the relevant IT Security Policies.

11.4 It was ascertained that not all the day-to-day processes and procedures are fully documented. This means there is a risk that should key staff leave or be absent for a considerable period of time there could be incorrect action and decisions taken by the team.

Recommendation 3: The IT Support team be required to review its documentation to ensure that all key processes and procedures are documented, version controlled and dated.

Recommendation 4: The IT Support team be required review and update all procedural documentation following the implementation of new systems, system upgrades and changes in processes.

12. Risk	Losses arising from unauthorised action by staff.
Risk Control Objective	Arrangements in place provide for safeguarding of NCH assets and interests from avoidable losses
Evaluation	<u>Limited Assurance</u>

13 The following matters were identified in reviewing the Key Risk Control Objective:

Risk: Unauthorised access to the network, affecting the availability, integrity and/or confidentiality of data.

13.1 NCH do not periodically receive logs of user activity for Network, Internet or email usage resulting in the primary method of identifying suspicious activity rests with NCC who do not necessarily know how to interpret NCH business needs.

Recommendation 5: NCH obtain monthly logs of User activity in the areas of Network, Internet and email usage and carry out a series of checks looking for actual or attempted misuse/abuse.

13.2 NCH does not possess its own Security Incident Management process but again relies on NCC to deal with this (indeed the Security policy as referred to above points NCH staff at NCC). This places NCH at risk of incorrect management of any incidents as business knowledge is unlikely to be correctly utilised.

Recommendation 6: NCH establishes its own Security Incident Management process and ensured that all suspected incidents are first notified to the relevant NCH personnel.

13.3 There are three members of the IT Team with partial administrator Network access but their rights and abilities are not documented and indeed are not known in full detail. This places NCH at risk of incorrect or inefficient action being taken by those staff.

Recommendation 7: The exact details of the partial administrator access rights granted to NCH staff be documented and held by both NCH and NCC.

13.4 There is no formal process of reviewing whether or not all User access rights granted are still necessary (although the IT Team do their best to review users they do not have detailed knowledge of the individual roles). There is therefore a risk that users retain access to systems and data that they have no authorised business need to access.

Recommendation 8: All Managers be required to carry out a review of all their staff system access requirements for their current role. This review be carried out on an annual basis (or more frequent if NCH deem necessary).

Risk: The network is disrupted, or data is lost, due to computer malware or hacking activity.

13.5 NCC operates effective Firewall and DMZ controls so no issues arise

Risk: The network is disrupted, or data is lost, due to the failure or network devices and inadequate recovery procedures.

13.6 NCH have not advised NCC of their prioritised requirements for the restoration of computer systems in the event of a disaster occurring. Currently, only the housing management system will be restored urgently and all other systems may take weeks to restore thus placing NCH at risk of serious business disruption.

Recommendation 9: NCH completes its Business Continuity Plan (which includes Disaster Recovery arrangements) as soon as possible and negotiates appropriate timescales for restoration of services by NCC. In addition NCH should ensure that it is involved in the Disaster Recovery testing programme on a periodic basis.

Risk: Networks are properly managed, with controls existing over error reporting and clearance, external connections and internet/email access.

13.7 See paragraph 13.1 above regarding the production and review of logs.

13.8 The change control process operated in conjunction with NCC is currently not operating correctly meaning that any appropriate impact on any changes made to network or systems may not be known or identified.



Recommendation 10: NCH be required to ensure that the change control process is operated correctly and effectively.
