

Final Audit Report

NCH Risk Management

Contents of Report		Page
1	Introduction and Background	2
2	Audit Approach	2
3	Objective	2
4	Main Conclusions.....	3
5	Findings in Detail	4
6	Action Plan.....	9
7	Glossary of Terms.....	12
	Appendix 1.....	13

Contact Details:		
Head of Risk & Audit Services	Shail Shah	54050
Audit Manager	Mick Ahern	54853
Auditor	Andrew Willson	54822

Document title:	NCH Risk Management Audit Report
Issue Date:	21 February 2008
Issued to:	Julie Crook, Director of Finance ICT & Governance Steve Everson, Interim Director of Finance
Copied to:	



1 Introduction and Background

- 1.1 A review of the arrangements in place for Risk Management was undertaken as part of the Council's rolling programme of NCH audits.

2 Audit Approach

- 2.1 The scope of the audit covered:
- Risk Management Framework
 - Risk management papers and reports
 - Risk management plans
 - Risk management risk registers
- 2.2 The Audit was undertaken by way of discussion with the Interim Director of Finance, business users and also by examination of pertinent documentation and where necessary testing and verification of such records.

3 Objective

- 3.1 The objective of the review is to provide assurance or otherwise that risk management is embedded into the working practices of NCH, according to best practice, thus providing increased confidence in NCH achieving its desired business objectives.

4 Main Conclusions

- 4.1 The Risk Management Framework (RMF) last revised in March 2007, provides for a comprehensive risk management foundation, detailing risk management policy, responsibilities, culture, management activities and the risk management cycle of events. However, the framework has not been approved by the Strategic Board, which is their responsibility to do so, as stated in the Framework.
- 4.2 The principal risk management activities identified in the RMF are not currently practiced and this was recognised within the report of the Interim Director of Finance on risk management, 3 December 2007, that states “the Risk Management Strategy and Risk Register are not fully developed” and that “our approach to risk management to date does not meet best practice.”
- 4.3 Embedding risk management into the culture of an organisation in a way which effectively supports the delivery of its objectives requires significant commitment and should be regarded as a project in its own right. A project plan, adequately resourced, lead by a dedicated project leader does not exist and should be established. Key plan milestones might include: updating the RMF, refreshing the corporate risk register, running risk management awareness briefings for senior management, running risk management workshops for staff, potentially adopting and implementing bespoke risk management software, introducing changes in risk management procedures to ensure best practice is assured and keeping senior management aware of emerging economic, financial, and technological risks, amongst others.
- 4.4 Best practice recommends that key risks are reviewed at the highest level on, typically, a quarterly basis. Risk management activities, detailed in the RMF (paragraph 4.7.1) calls for the “Key Risks in conjunction with the Business Plan and Delivery Plan to be reviewed annually” by the Strategic Board and the “review and update of Operational Risk Registers by Executive Management Team “at least once a year”.
- 4.5 An effective risk commentary in a management report or plan should provide information that contributes to the quality of management decisions arising from the report. It should provide risk information that is pertinent to the acceptance or not of the recommendations in the report. Current NCH business case risk assessments only attempt to identify the key risks, their ratings and mitigations. Assessments should provide a clear decision on the need or not for new risk management responses or quantify the upside of risk taking, in order to achieve important and significant benefits.

- 4.6 There are no plans in place at NCH to introduce formal risk management into project management methodologies, currently practiced, partnerships, or for large contracts of supply. To be fully effective, risk management should be applied to all major programmes of work as well as business plans. The most significant benefit is that it increases the probability of delivery, according to plan. For projects it does this by bringing project management and governance focus onto the most significant threats (risks) facing project implementation and the achievement of project objectives, outputs and outcomes. This ensures that risks receive the necessary attention and resources to mitigate their impact. Research has found that most late or partially delivered project outcomes were caused by factors (risks) that could have been predicted.

5 Findings in Detail

Risk Management Framework

- 5.1 The Risk Management Framework (RMF) details risk management activities, responsibilities and monitoring and review. However, the duties and tasks outlined for each body are inconsistent. For example:
- the Risk Management Panel is charged with monitoring operational medium and high risk scores on a quarterly basis before presentation to the Executive Management Team, but who review and update the registers potentially only once a year;
 - “the Audit Committee monitor the impact of new risks” (4.7.1) although this is not reflected in their responsibilities (4.8);
 - it is the Head of Performance and Best Value that produces the key (corporate) risk register for review by the Board on an annual basis (6.1).
- 5.2 We conclude, on the basis of our testing, that the mandatory requirement to develop a risk mapping process that is clearly linked to the activities and targets set out in the Corporate Strategy is not fully embedded into working practices. Following on, the requirement to assess the inherent risk of each activity, measure its potential impact on the organisation and evaluate the controls in place aimed at managing each risk, is not embedded into working practices.
- 5.3 The RMF does not describe a procedure for escalating risks according to their risk ratings. Risks identified at a departmental/service level that have the potential to impact at the corporate level need to have their profile raised.

Recommendations

- R1 *The responsibilities assigned to the various bodies identified in the RMF should be reviewed and clarified.*
- R2 *The RMF should describe the procedure for escalating risks.*
- R3 *The RMF should be approved by the Strategic Board on the recommendation of the Audit Committee.*
- R4 *The Board should review the key (corporate) risks that threaten business priorities and other off-plan risks (e.g. finance, reputation, statutory requirements, large scale emergency, etc) on a quarterly basis.*

Responsibilities

- 5.4 The Risk Management Panel identified in the RMF and nominated to play a key role in championing and embedding risk management across the Company had not been established.
- 5.5 The Audit Committee also have a key role to play in the risk management process by setting the risk appetite of the Company, recommending targets, limits and controls etc, and, therefore, should be familiar with current best practice.

Recommendations

- R5 *The Risk Management Panel should be established. The Company Secretary could potentially chair the Panel with nominated senior managers acting for each director of the Company.*
- R6 *The terms of reference for the Risk Management Panel should include:*
- *ensuring corporate and other key risks are reported quarterly to the Board;*
 - *production of an annual risk report*
- R7 *The Audit Committee should receive risk management awareness training.*

Documentation

- 5.6 The report of the Interim Director of Finance on risk management, 3rd December 2007, recognised that the “Company is required to have in place a Risk Management Policy within the Board Members’ Handbook and Standing Orders clearly state that a Risk Register is required. However, these key documents need to be updated and formally adopted in the context of a RMF for the Company.”

Recommendation

R8 *The Board Members Handbook should include a Risk Management Policy.*

Risk Registers

- 5.7 A corporate risk register and some business area risks registers have been established. All have a risk register date of February 2007, however, the RMF states that red risks should be reviewed on a quarterly or more frequent basis, yellow risks on a quarterly basis and green risks on an annual basis.
- 5.8 Risk registers have been established for many but not all business areas, identified in the draft delivery plan 2007-2009. Risk registers do not exist for: Estate Services, Rent Collection, Capital Programme and Revenue Budget. These areas are all finance based and as such are inherently high risk. Specifically, Rent Collection is a business area where a full risk assessment should be done.
- 5.9 The report of the Interim Director of Finance on risk management, 3rd December 2007, recognised that “the Risk Management Strategy and Risk Register are not fully developed”.

Recommendations

- R9 *The corporate and business area risk registers should be reviewed and updated to reflect current risks, ratings and mitigations.*
- R10 *On an ongoing basis, risks should be reviewed according to the requirements of the RMF.*
- R11 *Risk registers should be established for all business areas that have declared business priority outcomes.*
- 5.10 There are key business functions whose objectives are not necessarily recognised within delivery plans, for example, information technology, business continuity and statutory requirements. They are effectively ‘off plan’ objectives (other duties, responsibilities and challenges) but they need to be recognised and their associated risks determined and managed.

Recommendation

- R12 *All business risk registers should include the risks aligned to key ‘off plan’ objectives (other duties, responsibilities and challenges).*

- 5.11 None of the risks identified in the departmental risk registers have an associated risk owner. An owner acquires specific responsibilities that are designed to ensure the organisation and its activities are adequately protected from the negative consequences of the “owned” risk.
- 5.12 An objective evaluation of existing risk registers (corporate and business functions) was undertaken to gauge their consistency and rigour. The evaluation was based upon 11 criteria, with each criterion having a sliding scale of 1 (poor) to 10 (excellent). This approach was used to evaluate the Nottingham City Council risk registers during the 2007/2008 annual planning process. The overall average attained by NCH was 44%. A breakdown of the criteria used is detailed at Appendix 1. The results are encouraging, but we conclude that formal risk management training, at all levels, should be embarked upon to raise better understanding of risk management generally.
- 5.13 A 5x5 risk matrix has been adopted to “be used across the Company to measure risk” (RMF) however, the risk registers for Vacant Property Management and Tenancy Estate Management have used a 7x7 matrix.
- 5.14 All departmental risk registers:
- fail to describe the impact of a risk should it materialise;
 - fail to nominate a risk owner, either collectively or individually;
 - fail to provide a residual risk rating;
 - fail to provide an “in operation” date for risk responses.

Recommendation

- R13 All departmental risk registers should be completed to include:*
- *a description of the impact;*
 - *the owner of each risk (an owner should be an individual; not a group or team);*
 - *a residual (target) risk rating;*
 - *an “in operation” (target) date for risk responses.*

Embedding Risk Management

- 5.15 Work on reviewing the underlying approach to the management of risk has been started by the Interim Director of Finance with a discussion of the principles of risk management with senior managers who will be expected to take the lead. However, to achieve an organisational culture of well thought-through risk taking and innovation, embedded in day to day management processes, risk management needs to be

championed by an officer who, with adequate resources and the backing of the Strategic Board, can influence its pace and direction. Risk management, when fully practiced, should include assessments of key business priorities, projects, partnerships and large scale contracts.

Recommendations

- R14 Consideration should be given to the appointment of a corporate risk officer, potentially on a full time basis for at least an interim period, to ensure identified risk management critical success factors are established and a plan of action is prepared and implemented.*
- R15 A project plan should be prepared that identifies the tasks and milestones in embedding risk management fully into the normal working routines and activities of NCH.*
- R16 The project plan (above) should recognise that all staff should be given appropriate training and guidance to enable them to take responsibility for managing risk within their own working environment.*
- R17 The project plan (above) should recognise the need to introduce formal risk management into project management, partnerships and large contracts aligned to the principles adopted for business risk management where it is appropriate to do so. It is recognised that this objective may have to be deferred until business risk management has taken a foothold.*

5 Action Plan

Ref	Recommendation	Priority	Management Response	Responsibility and Target Date
R1	The responsibilities assigned to the various bodies identified in the RMF should be reviewed and clarified.	M	Agreed. Work on review of the RMF and Registers has commenced with a target for Board approval of updated documents in May.	Director of Finance. May 2008
R2	The RMF should describe the procedure for escalating risks.	M	As above	Director of Finance May 2008
R3	The RMF should be approved by the Strategic Board on the recommendation of the Audit Committee.	H	As above	Director of Finance May 2008
R4	The Board should review the key (corporate) risks that threaten business priorities and other off-plan risks (e.g. finance, reputation, statutory requirements, large scale emergency, etc) on a quarterly basis.	H	Agreed	Director of Finance May 2008
R5	The Risk Management Panel should be established. The Company Secretary could potentially Chair the Panel with nominated senior managers acting for each director of the Company.	M	Agreed	Company secretary May 2008
R6	The terms of reference for the Risk Management Panel should include: <ul style="list-style-type: none"> ensuring corporate and other key risks are reported quarterly to the Board; production of an annual risk report. 	M	Agreed	Company Secretary May 2008
R7	The Audit Committee should receive risk management awareness training.	H	Agreed. Training timetable for Board to be finalised.	Director of Finance

Ref	Recommendation	Priority	Management Response	Responsibility and Target Date
				May 2008 (provisionally)
R8	The Board Members Handbook should include a Risk Management Policy.	L	Agreed	Company Secretary June 2008
R9	The corporate and business area risk registers should be reviewed and updated to reflect current risks, ratings and mitigations.	H	Agreed	Director of Finance May 2008
R10	On an ongoing basis, risks should be reviewed according to the requirements of the RMF.	M	Agreed	Director of Finance May 2008
R11	Risk registers should be established for all business areas that have declared business priority outcomes or other duties, responsibilities and challenges.	H	Agreed	Director of Finance May 2008
R12	All business risk registers should include the risks aligned to key 'off plan' objectives (other duties, responsibilities and challenges).	M	Agreed	Director of Finance May 2008
R13	All departmental risk registers should be completed to include: <ul style="list-style-type: none"> • a description of the impact; • the owner of each risk (an owner should be an individual; not a group or team); • a residual (target) risk rating; • an "in operation" (target) date for risk responses. 	H	Agreed	All Directors, led by Director of Finance May 2008
R14	Consideration should be given to the appointment of a corporate risk officer, potentially on a full time basis for at least an interim period, to ensure identified risk management critical success factors are established and a plan of action is prepared and implemented.	M	This will be a product of the work currently in progress to review the RMF and registers. The role is likely to be included within that of the Company Secretary	Director of Finance May 2008

Ref	Recommendation	Priority	Management Response	Responsibility and Target Date
R15	A project plan should be prepared that identifies the tasks and milestones in embedding risk management fully into the normal working routines and activities of NCH.	H	Agreed	Director of Finance May 2008
R16	The project plan (referred to above) should recognise that all staff should be given appropriate training and guidance to enable them to take responsibility for managing risk within their own working environment.	M	Agreed. Completion of the training to follow over a probable 2-3 month period.	Director of Finance August 2008
R17	The project plan (referred to above) should recognise the need to introduce formal risk management into project management, partnerships and large contracts, aligned to the principles adopted for business risk management where it is appropriate to do so. It is recognised that this objective may have to be deferred until business risk management has taken a foothold.	L	Agreed	Director of Finance September 2008

Signed..... Date.....

(Service 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.

Appendix A

Risk Register Evaluation Form

Purpose: To evaluate the content of the risk register against the NCH Risk Management Framework

Service Area:
Service Director:

- 1. The Risk Register conforms to the current published standard**
(Poor) 1 2 3 4 5 6 7 8 9 10 (Excellent)

- 2. The risk register review date is not greater than 3 months from today's date**
(Poor) 1 2 3 4 5 6 7 8 9 10 (Excellent)

- 3. All risks relate to priority outcomes/business objectives/other declared duties, responsibilities or challenges**
(Poor) 1 2 3 4 5 6 7 8 9 10 (Excellent)

- 4. All risks are operationally focused**
(Poor) 1 2 3 4 5 6 7 8 9 10 (Excellent)

- 5. A named individual is identified as the risk owner for each risk determined**
(Poor) 1 2 3 4 5 6 7 8 9 10 (Excellent)

- 6. Risks described encompass the threat and impact on the declared objective(s) (cause and consequence)**
(Poor) 1 2 3 4 5 6 7 8 9 10 (Excellent)

- 7. Financial risks are subject to numerical diagnosis/quantification**
(Poor) 1 2 3 4 5 6 7 8 9 10 (Excellent)

- 8. Prevailing red risks have been addressed with additional mitigating factors**
(Poor) 1 2 3 4 5 6 7 8 9 10 (Excellent)

- 9. Prevailing blue and green risks are tolerated (unless referred to in the risk summary as being particularly significant)**
(Poor) 1 2 3 4 5 6 7 8 9 10 (Excellent)

- 10. Additional mitigations/countermeasures are reasonable, relevant and include target dates**
(Poor) 1 2 3 4 5 6 7 8 9 10 (Excellent)

- 11. Residual risk ratings are reasonable and within tolerable limits**
(Poor) 1 2 3 4 5 6 7 8 9 10 (Excellent)