



## **NCH Risk Management Framework**

**May 2008**

# **Risk Management Framework.**

## **1. GENERAL INTRODUCTION AND BACKGROUND**

### **1.1 Introduction**

**1.1.1** Risk is inherent and unavoidable in every activity that an organisation undertakes. The aim of effective risk management is to manage risks and their potential for damage down to an acceptable level. Successful organisations manage risks to the delivery of their core business objectives explicitly and effectively.

**1.1.2** To enable Nottingham City Homes (NCH) to achieve this, NCH needs to understand the risks that it faces and how it is currently controlling these risks. NCH must ensure that all staff understand the importance of risk management as part of the day to day decision-making process.

**1.1.3** The Risk Management Framework has been developed in line with the City Council's own framework and will be put to Board Members for approval. It is intended that as soon as the Framework is ratified by Members the process for implementing and embedding risk management across the Company will be accelerated.

**1.1.4** The overall responsibility for risk management within the Company lies with the Board and although the Audit Committee and senior managers play an important role in the management and review of risk management, the Board can not avoid or delegate its overall responsibility.

**1.1.5** The implementation of risk management within NCH will be followed by a process of updating all Service Area Risk Registers, introducing additional Service Area and Directorate Risk Registers as well as integrating All the Company's Key Risks into the Corporate Risk Register.

### **1.2 Background**

**1.2.1** A more formal approach to risk management was introduced in the United Kingdom, across both the private and public sectors, following the publication of the Combined Code 'Principles of Corporate Governance and Code Provisions' (issued June 1998), and the

- 1.2.2** There have been a number of other reports published on the subject of corporate governance that incorporate formalised risk management, including those by Cadbury, Greenbury, and Langlands.
- 1.2.3** Whilst most of these reports originated in the private sector they have much to offer in the public sector also. These reports have been added to by the Audit Commission's publication "Worth the Risk". This document forms the basis of current best practice in the sector and has been used to develop this Framework.
- 1.2.4** Corporate governance can be described as the systems which public sector organisations use to direct and control their operations and relate to their communities. Good corporate governance can provide confidence that an organisation maintains the highest possible standards in delivering their services.
- 1.2.5** As part of its objective to become an excellent organisation, NCH will be seeking to emulate best practice in the fields of corporate governance and controls assurance. Risk management is a key element of both and this framework seeks to ensure that the Company can operate a robust control environment.
- 1.2.6** The City Council has to comply with various statutory requirements which include corporate governance and risk management issues, notably 'The Accounts and Audit Regulations 2003 (Amended 2006)' and the requirement to publish a Statement of Internal Control (SIC) in its annual financial statements. Although NCH functions independently to City Council, it remains allied in its housing and other corporate strategies and should therefore endeavour to adhere to these requirements.

## 2. PURPOSE AND SCOPE

### 2.1 Purpose

2.1.1 The Company's vision is that all significant risks which may prevent NCH from achieving its objectives are identified, assessed and cost effectively managed, as part of NCH's performance management process.

2.1.2 The purpose of the Risk Management Framework is to establish a consistent basis for identifying, measuring, controlling, monitoring, managing and reporting the Company's strategic, operational and project/partnership risks.

2.1.3 The Framework, therefore:

- Is based on NCH's corporate objectives, which are supported by the service area objectives;
- Identifies the risks which may prevent NCH achieving its objectives and targets;
- Identifies and assesses what NCH is doing to manage the risks it has identified;
- Identifies what systems are in place to record and monitor the management and assurance processes;
- Reviews what actions have been taken to address any gaps; and
- Identifies what systems are in place to report on risks and risk management.

2.1.4 The Framework has the following 3 main elements:

- **Risk Strategy** – sets out why risk management is important for the Company;
- **Risk Management Policy** – details the risk management system of the Company; and
- **Priority Action Plan** – identifies the priorities for risk management activities in a financial year.

2.1.5 The Framework sets out what risk management means for NCH. It defines the appetite that NCH has for risk and explains the risk language that NCH will be adopting across the organisation. It specifies who is responsible for managing risk, the processes undertaken to embed risk management into the Company's culture.

## **2.2 Scope**

- 2.2.1** For the purpose of this Framework, definitions will be applied, in line with the Risk Management Standard issued by the Institute of Risk Management. These definitions are set out in Appendix A - Terms and Definitions.
- 2.2.2** NCH has established its corporate objectives, summarised in Appendix B - Key Objectives of Nottingham City Homes, and it is these objectives that the Risk Management Framework will apply to.
- 2.2.3** NCH will ensure that all statutory requirements and regulatory guidance relating to risk management is followed.

### **3. RISK MANAGEMENT STRATEGY**

#### **3.1 Introduction**

**3.1.1** The purpose of the strategy is to set out why risk management is important, in what context it should be seen and why it needs to be an intrinsic part of the way in which the organisation operates now and in the future.

**3.1.2** All organisations face uncertainty which both exposes the organisation to risk and presents them with opportunities. Effective risk management increases the probability of success and reduces both the probability of failure and the uncertainty of achieving the organisation's overall objectives. It is not a panacea but does provide a rigorous and robust framework for the organisation to focus on what it needs to measure, monitor and manage if it is to deliver its core objectives.

**3.1.3** In summary, the successful implementation of a robust risk management process at strategic, project and operational level is vital to achieving the Company's objectives.

#### **3.2 What is Risk and Risk Management?**

**3.2.1** For a public body such as NCH risk can be described as:

***'Anything that poses a threat to the achievement of the Company's objectives and programmes or the delivery of services to the residents and communities of Nottingham'.***

A definition of risk in line with the IRM Risk Management Standard is included in section 6.1.1.

**3.2.2** Risks can come from inside or outside NCH, and may include financial loss, physical damage to people or buildings, client dissatisfaction, unfavourable publicity, failure of equipment, or fraud. Failing to take advantage of opportunities may also have risks for the Company,

**3.2.3** There is no such thing as a risk-free environment, but many risks can be avoided reduced or eliminated through good risk management. Good risk management also takes advantage of opportunities while analysing and dealing with risks

- 3.2.4** Taking advantage of new opportunities can also mean NCH has to deal with different types of risks. However, failing to take advantage of new opportunities may leave the Company facing bigger risks in the future, e.g. not bidding for external funding, or not publicising successes.
- 3.2.5** Therefore, some risks should not necessarily always be avoided. However, this should not mean that NCH makes poorly thought through decisions which may cause a loss of confidence, damage the Company's reputation or impact on its finances. If risks are identified and managed effectively, they can allow the Company to take opportunities for improving services.
- 3.2.6** Risk management is something that managers do every day as part of their normal work, although it may not always be written down and managers may not use a formal procedure to make their final decision. Risk management can be explained as a tool for managers to use so that they are able to identify, evaluate and manage both risks and opportunities in a logical and consistent way.
- 3.2.7** Risk management should be considered as a continuous process, which evolves as NCH gains more understanding of the risks and opportunities facing it and how to manage these effectively.
- 3.2.8** Risk management consists of a number of elements which should be considered and applied regularly during the course of the year as part of NCH's cycle of performance management and improvement processes, including:
- Understanding NCH / Directorate / service area objectives;
  - Identifying and assessing the risks facing them;
  - Assessing the actions in place to manage the risks;
  - Taking action to improve, monitor and learn from experiences.
- 3.2.9** Risks according to how they may affect NCH as it delivers its services can be classified as follows:
- **Strategic (Corporate) risks** - risks which may affect the Company's ability to achieve its plans.
  - **Project (Programme) risks** – risks that may impact on the organisation's ability to complete projects within the original budgets and timescales or deliver the required outputs; and

- **Operational (Service) risks** – risks which may prevent the Company delivering its core services, e.g. lack of staff, damage to buildings, equipment failure.

Various Examples of these risks are included in Appendix E - Risk Checklist.

**3.2.10** In most cases these risks can be further classified as:

- **Reputational risks** - risks that may undermine the confidence that NCH's partners, customers, staff and the public have in it, e.g. adverse news articles; and
- **Financial risks** – risks which may cause a breakdown in NCH's financial systems e.g. fraud.

### **3.3 Benefits from Risk Management**

**3.3.1** Good risk management is forward looking and helps to improve business decisions and manage performance. It is not only about avoiding or minimising losses, but also about dealing positively with opportunities.

**3.3.2** Risk Management is an essential and important activity as it:

- Is an intrinsic part of good management, not an add on activity;
- Focuses on what is important in achieving the organisation's / project's objectives;
- Promotes better decision making, planning and prioritisation by a comprehensive and structured understanding of Company activity and the volatility of our business;
- Assists project management by aiding in the identification of opportunities and threats to the project;
- Promotes greater and clearer accountability within the Company; and
- Promotes stakeholder confidence in the organisation.

**3.3.3** In addition to fulfilling statutory requirements there are many benefits associated with ensuring that risk management is established and embedded within the Company, notably:

- Assisting the Company in achieving its objectives at all levels within the organisation and within the many partnerships the Company is involved in;

- Providing an early warning system, that alerts officers to undertake preventative actions and reduces surprises;
- Targeting resources at areas and issues of greatest risk where the organisation's or project's objectives are most under threat;
- Promoting informed risk taking and decision making at all levels of the organisation;
- Providing a better understanding of the risks and exposures faced by the organisation;
- Promoting greater ownership of risks as part of a robust system of internal control;
- Providing an environment that enables and encourages innovation;
- Allowing managers to focus on the issues that really matter;
- Spending less management time within the organisation on operational issues;
- Focusing Managers on doing the right things, in the right way; and
- Increasing the chances that new developments and projects can be delivered on time, in accordance with the planned programme and within budget.

### 3.4 Developing the Culture and Approach to Risk Management

3.4.1 Nottingham City Homes must develop a culture of risk management at all levels and in all parts of the organisation so that it forms part of the every day fabric of the organisation. The challenge is for the Company to move:

<b>FROM:</b>	<b>TO:</b>
Risk as individual hazards	Risk in the context of strategic objectives
Focus on all risks	Focus on critical risks
Risks with no owners	Defined risk responsibilities
Ad hoc out of date risk registers	Dynamic and relevant electronic risk registers
Haphazard risk quantification	Consistent measurement & monitoring of risks
Risk is not my responsibility	Risk is everyone's responsibility
Risk management as limiting	Strategic approach to informed risk taking

3.4.2 Risk management is one tool to improve performance. It must be part of a coherent system of management within the organisation with the following key elements:

- Service planning (Delivery Plan, Project Plans);
- Partnership plans (Service Level Agreements);

- Financial planning and management (Medium Term Financial Plans, Annual Budgets (Capital and Revenue), external funding, budget monitoring);
- Risk management (Risk Management Framework, Risk Registers, Statement on Internal Control and Business Continuity Plans);
- Performance management (Service Improvement Plans, Performance Framework, Performance Plans);
- Annual appraisal and personal development (Appraisals, training and development needs, mentoring).

**3.4.3** Performance monitoring and reporting should be undertaken in an integrated way so that objectives are planned, resources, risk assessed and delivery managed proactively as a chain of connected events rather than a series of uncoordinated activities.

**3.4.4** The majority of organisations use a system of risk registers in order to maintain information on all the identified risks relating to specific objectives (Strategic, Directorate or service area) or projects.

**3.4.5** The system of risk registers is the organisation's 'intelligence network' of information about risks and how they are being managed. Setting up a system of risk registers is only one part of the risk management process. In order to achieve real benefits from implementing risk management, it is important that the risk registers are reviewed and kept up to date on a regular basis.

**3.4.6** The critical success factors for effective risk management include:

- Clearly identified responsibilities for senior management and Board Members;
- An agreed and effective Risk Management Framework;
- The existence of an organisational culture which supports well thought-through risk taking and innovation;
- Management of risk is embedded in day to day management processes and consistently applied;
- Management of risk is linked to the achievement of strategic and operational objectives; and
- Risks are actively monitored and regularly reviewed on a constructive 'no blame' basis.

**3.4.7** The critical success factors associated with the Company's priority actions are included in the Risk Management Action Plan, see section 5.1.

## **3.5 What is an Acceptable Risk**

**3.5.1** As a general principle, NCH will seek to eliminate and control all those risks which:

- Have a high potential for incidents to occur;
- Would have a substantial adverse financial impact;
- Would cause loss of public confidence in the Company, and consequently the City Council, and/or its partner organisations;
- May prevent NCH from meeting its obligations under the Management Agreement with the City Council; or
- May stop NCH from assisting the City Council to carry out its statutory functions.

**3.5.2** Risk cannot be eliminated completely and NCH recognises that it is impossible to eliminate all risks and therefore risk needs to be reduced to an acceptable level. What constitutes an acceptable level of risks will be subject to discussion by the Board.

**3.5.3** NCH will always try to reduce or eliminate risks wherever possible, but it needs to strike the right balance between how much it costs to manage or eliminate risks and taking no action. For example, the costs of eliminating risks in a system may be more than the amount of money the Company may lose if the system were to fail. In these circumstances, NCH would want to ensure that there were sensible precautions taken to manage the risks, but that these were balanced against what it would cost if the system were to break down.

**3.5.4** NCH's objective is to make sure that the most cost-effective controls are in place for each risk, and that managers have considered the cost against the benefit of the control. This means that certain risks will always have an impact on the organisation because the cost of reducing the risk is higher than the cost of the risk actually occurring.

**3.5.5** Whilst the concept of a risk appetite as being the extent to which NCH would be prepared to take additional risks in order to achieve its objectives is relatively easy to grasp, defining it is more difficult and the following matters need to be taken into consideration.

**3.5.6** NCH is a company with the principal aim of providing an excellent service to its customers, the current and prospective Council tenants and leaseholders of Nottingham. It would be inconsistent with this mission deliberately to take risks in order to secure high financial returns, for instance through its asset management team, in the way that commercial companies do.

- 3.5.7** NCH works in a sector of considerable political and social importance, where changes in government policy and in the marketplace for social housing can repeatedly impose the need for innovation and change and may also result in significant financial risk.
- 3.5.8** Changing nothing could itself be a high-risk strategy. NCH must live with the risks inherent in defining and implementing change doing what it can to avoid, minimise and control them and their impact.
- 3.5.9** Systems that NCH puts in place should therefore be flexible enough to encourage innovation and imaginative use of its limited resources, subject to any legal requirements, in order to deliver better services to local residents.
- 3.5.10** The Risk Management Policy describes the system for identifying, assessing and managing risks within NCH. It describes when and how the Company would be willing to accept risks before any action would be taken to manage them.

### **3.6 Who is responsible for Risk Management?**

- 3.6.1** NCH Executive Directors and senior managers are responsible for managing their services. They are therefore responsible for identifying, assessing and managing the risks associated with planning, delivering and monitoring service delivery.
- 3.6.2** The individual responsibilities for risk management lie with the Chief Executive and the five Executive Directors within the following Directorates:
- Finance, ICT and Governance;
  - Organisational Development;
  - Strategy and Partnerships;
  - Housing Services; and
  - Property Services.
- 3.6.3** In order to assist Executive Directors and senior managers implement a consistent and structured risk management process across NCH, in line with the Risk Management Strategy and Policy, the Director of Finance, ICT and Governance has been assigned overall responsibility for risk management and the Company Secretary as been appointed as the Company's Corporate Risk Officer.
- 3.6.4** NCH as a whole is accountable to the City Council through a range of monitoring and review processes. The City Council needs to be

### **3.7 Strategic Risk Management**

**3.7.1** NCH recognises the important contribution that effective and explicit risk management can make to the achievement of objectives at a strategic, project / partnership and operational level.

**3.7.2** Risk management does not exist to stifle innovation or risk taking itself but to demonstrate that the organisation clearly identifies the risks to its objectives, measures these, monitors the systems in place and manages risk in a proportionate way.

**3.7.3** Risk management activities must:

- Relate to what the organisation state its wants to achieve;
- Support effective delivery of services, projects and partnerships;
- Be targeted at critical risks;
- Be proportionate to those risks;
- Not seek to stifle innovation or promote the avoidance of risk;
- Track and report critical risks to Members in a transparent manner;
- Be integrated into everyday management of the organisation;
- Act in concert with planning, resource allocation and performance management activities; and
- Meet regulatory requirements.

**3.7.4** There should be evidence to show that risks have been considered when key Company decisions are made, including:

- Reports to Board and Committees
- Projects and Programme Initiatives;
- Policy and Strategy Documents; and
- Key Executive Management Team (EMT) decisions.

**3.7.5** The accompanying Risk Management Policy sets out the detail of the Company's risk management system. It details how risks are identified, quantified, how options to deal with them are identified, how decisions on risk management are taken, implemented and evaluated. Executive Directors, Service Area Managers/RROs, other managers and other staff are primarily responsible for ensuring that the Risk Management Framework is implemented and further embedded with the Company's structure.

### **3.8 Business Continuity**

- 3.8.1** Business continuity management is a process that helps to manage the risks to the smooth running of an organisation or the delivery of a service. Thus it ensures that the organisation can continue in the event of a disruption, or recover to an acceptable level of operation within an acceptable timescale.
- 3.8.2** This can be achieved by analysing the organisation's processes so that plans can be put in place to eliminate, mitigate or reduce the risks to acceptable levels. Also, planning alternative methods of operation to be utilised in the event of a disruption will increase service delivery resilience.
- 3.8.3** In particular, Business Continuity Plans should prioritise which functions are most critical to the organisation and alternative means of establishing these in a managed way in the event of a disruption.

### **3.9 Developing the Progress – Training and Education**

- 3.9.1** NCH is developing risk management on a formal basis and has identified the actions it needs to take to ensure that risks are considered in all key business and performance management processes.
- 3.9.2** However, NCH now needs to make sure that risk management is embedded throughout the organisation. Processes for monitoring and reporting of risks and the actions proposed need to be endorsed and approved by the Board before they are implemented.
- 3.9.3** Whilst those managers involved in producing risk registers, business plans, project management documentation etc, have an understanding of risk management, people outside of these processes may be unaware of what it is or how it impacts on their jobs.
- 3.9.4** Therefore, it is important that not only are people made aware of risk management, but also that there is a degree of succession planning in place to enable staff to develop skills and undertake some of the risk management processes.
- 3.9.5** Levels of training and education will differ depending on the needs of staff and available resources. Possible methods of improving awareness may include briefings to specific service teams and



## **4. RISK MANAGEMENT POLICY**

### **4.1 Introduction**

**4.1.1** The objective of any policy is to provide consistent guidance to people in the organisation. Derived from the Risk Management Strategy, it provides a set of guidelines and requirements that reflect culture and values, and are reviewed and changed as needed. The policy should be supported by robust and comprehensive processes and procedures.

**4.1.2** While the Risk Management Strategy is concerned with what we should provide and why i.e elements that will not change very often, the Risk Management Policy establishes how we will deliver the resulting portfolio of programmes and processes.

**4.1.3** The purpose of this policy document is to:

- Establish risk management processes to enable NCH to meet its corporate objectives (summarised in Appendix B - Key Objectives of Nottingham City Homes);
- Raise awareness of risk management and embed it in the culture of the Company;
- Establish the relative responsibilities for risk management within NCH and the procedure for escalating risks; and
- Instigate systems for monitoring, measuring and controlling risk and recording the rationale for decisions made.

### **4.2 Risk Management Process**

**4.2.1** All organisations face uncertainty which presents both risks and opportunities to an organisation. Effective risk management increases the probability of success and reduces both the probability of failure and the uncertainty of achieving the organisation's overall objectives. It is not a panacea but does provide a rigorous and robust framework for the organisation to focus on what it needs to measure, monitor and manage if it is to deliver its core objectives. In summary, the successful implementation of a robust risk management process at a strategic, project and operational level is vital to achieving the Company's objectives.

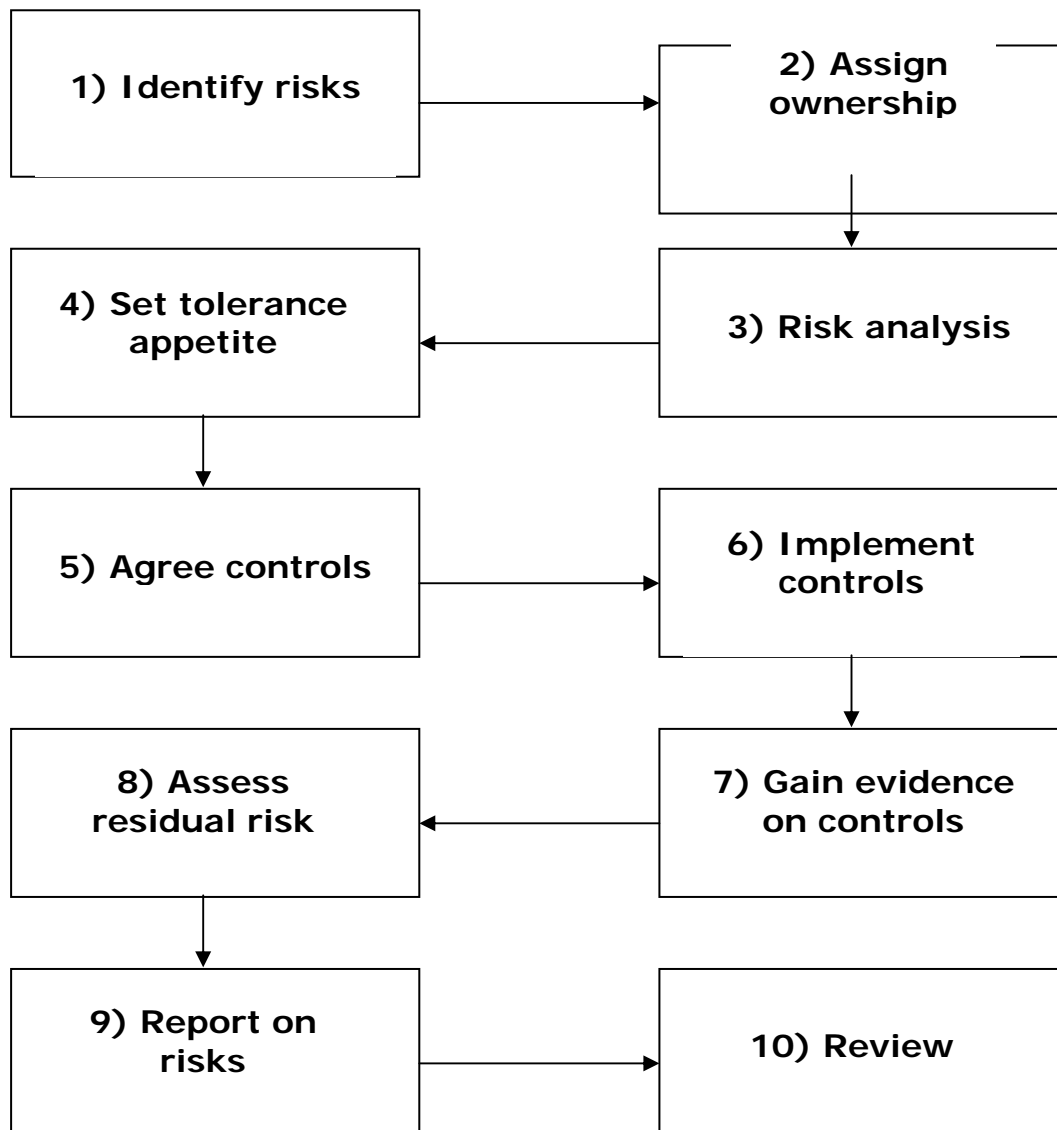
**4.2.2** Managing risk is a continuous process, which needs to be embedded into NCH's systems to aid decision making, accountability and systems improvement. Risk management is one element of an integrated approach to corporate governance.

**4.2.3** NCH has developed a risk mapping process that is clearly linked to the activities and targets set out in the Company's strategy

documents. NCH has assessed the inherent risk of each activity, measured its potential impact on the organisation and has evaluated the controls in place aimed at managing each risk. The terminology used in this framework complies with the IRM Risk Management Standard and the key definitions are recorded in Appendix A - Terms and Definitions.

**4.2.4** The Risk Management cycle assumes that there is clarity about what the strategic, project, partnership and operational objectives are. It is important to establish that everybody involved has a common understanding of what needs to be achieved. Organisations should not invest time in the Risk Management process if they have not already established clear objectives. Doing so will diminish the value that Risk Management can add as all activities will be based on a lack of clarity from the start.

**4.2.5** A ten step approach has been adopted in line with the approach of the City Council and the Risk Management Cycle is detailed more thoroughly in Appendix C - Risk Management Cycle.



- 4.3.1** The first stage of the process is to identify the risks facing NCH. In line with CIPFA/SOLACE guidance, the Company shall ensure that the Risk Management Framework is linked to business objectives and these objectives are identified as part of the annual business planning process. This process identifies key risks to be managed in terms of achieving objectives and resource requirements.
- 4.3.2** The individual responsibilities for risk management within NCH lie with the Chief Executive and the five Executive Directors of the following Directorates:
- Finance, ICT and Governance;
  - Organisational Development;
  - Strategy and Partnerships;
  - Housing; and
  - Property Services
- 4.3.3** NCH's system of risk registers is based on the Company's Directorate structure (excluding Chief Executive) and is supported by a number of individual Service Area Risk Registers. This is based on the assumption that Directorate only risk registers will lack sensitivity to many important organisational issues.
- 4.3.4** Executive Directors have overall responsibility for their Directorate and respective Service Area Risk Registers. The Risk Register Evaluation Form should be used by Executive Directors and Service Area Managers / Risk register Responsible Owners (RROs), to evaluate the content of their risk registers against the NCH Risk Management Framework. See Appendix D - Risk Register Evaluation Form.
- 4.3.5** The Service Area Risk Registers will focus on the risks affecting each individual service, although some of the risks may have an impact on whether the service area, or NCH meets, its objectives. Those service areas have been defined as:
- Access and Customer Care;
  - Allocations, Lettings and Voids;
  - Resident Involvement;
  - Housing Income Management;
  - Leaseholders;
  - Tenancy and Estate Management;
  - Supported Housing;
  - Stock Investment and Asset Management;
  - Contract Services;
  - Finance;
  - ICT;
  - Governance;

- Human Resources;
- OD and Learning;
- Health and Safety;
- Communications and Marketing;
- Business Improvement and Development; and
- Equality and Diversity.

**4.3.6** The risk registers should be developed by identifying risks in one of two main ways:

- Risk Management Workshops – attended by all relevant senior management and Service Area Managers/RROs; and
- Compilation and review of relevant service area business plans and/or Service Improvement Plans (SIPs) i.e. operational risks – process should involve input from all members of the management team and consultation with other key staff groups.

**4.3.7** Operational risks identified within service areas should be linked to the associated service improvement and delivery plans that have been established within those areas. This will ensure that risk management is seen as a key business driver and is embedded as part of the management culture.

**4.3.8** There are also a large number of ‘prompt lists’ available to help organisations categorise risk that should be used by Board Members, Executive Directors and Service Area Managers/RROs when establishing areas of most concern and the associated risks. A summary of prompts relevant to the Company are included in Appendix E - Risk Checklist.

**4.3.9** A nominated Service Area Manager, or Risk Register RRO, within each service area will be assigned the responsibility for maintaining and updating their respective Service Area Risk Register on an ongoing basis. A quarterly review of the registers should be formally signed off by managers/owners to confirm that they have considered their risks, made any changes required and allocated responsibility for required actions to individual officers.

**4.3.10** A nominated Risk Register Responsible Officer (RRRO) within each Directorate will be assigned responsibility for maintaining and updating a Directorate Risk Register. A bi-annual review of the register should be formally signed off by each RRRO to confirm they have been updated to reflect key risks included in the respective Service Area Risk Registers.

**4.3.11** Service areas may choose to establish and maintain risk registers at a lower level. In such cases, the Service Area Managers/RROs are still responsible for ensuring that all significant risks identified are fed into the Service Area Risk Registers

- 4.3.12** A Corporate Risk Register, maintained by the Corporate Risk Officer, will also be developed to identify the high level risks which could impact on NCH as a whole. The Corporate Risk Register will primarily report on risks associated with the achievement of the Company's strategic objectives, set out in the Delivery Plan, as well as any significant high level risks included in Directorate Risk Registers. Risk Register Responsible Officers will be required to ensure that significant high level Directorate risks are fed into the Corporate Risk Register on a timely basis.
- 4.3.13** All risks included in risk registers will be aligned to NCH's key objectives (summarised in Appendix B - Key Objectives of Nottingham City Homes). All risk registers will contain the following in relation to each risk:
- Description of the risk – separated by Company objective;
  - Description of the potential impact of the risk – with estimated costs where possible;
  - Description of the potential likelihood of the risk occurring;
  - Initial Impact and Likelihood ratings and the related risk score;
  - The 'Risk Owner' – the officer responsible for each risk;
  - Summary of the controls in place to mitigate and manage the risk;
  - Residual Impact and Likelihood ratings and the final risk score; and
  - A record of the Service Area Manager/RRO (or RRRO) responsible for the Service Area (Directorate) Risk Register and evidence of its quarterly (bi-annual) update and review.
- 4.3.14** The Board will review the Corporate Risk Register and the Key Risks facing the Company annually in conjunction with the Business and Delivery Plans.
- 4.3.15** The Audit Committee will focus their attention on the Key Risks facing the Company and shall review the Corporate Risk Register on a quarterly basis.
- 4.3.16** The Audit Committee will also review Directorate Risk Registers on a six monthly basis, making comments and updating them as required, to confirm their acceptance of the risks included in the registers as well as the actions in place to manage them.
- 4.3.17** Key triggers for significant changes to risk registers will be new or changing regulations, implementation of new projects, high staff turnover, changes in the external environment or audit reviews and updates may take the form of new risks, changes to controls, additional control or changes to risk ratings and scores. These shall be considered by the Audit Committee as part of their six monthly review of Directorate Risk Registers and quarterly review of the Corporate Risk Register.

- 4.3.18** The Audit Committee will review the Risk Management Framework in advance of the final Board meeting of the financial year to ensure that it remains up to date and reflects what is happening across the organisation. The Board will then subsequently approve the Framework before the start of the following financial year.
- 4.3.19** The Director of Finance, ICT and Governance will report quarterly to the Executive Management Team and the Audit Committee on risk management.
- 4.3.20** The Director of Finance, ICT and Governance will also report annually to the Board on the risk management process within the Company and the work of the Risk Management Panel.
- 4.3.21** The City Council has to produce a Statement of Internal Control (SIC) every year, which is an assessment of the systems the Council has in place to control and manage the services they provide. This Risk Management Framework within NCH will provide assurance to the Council that risks are being properly managed and assist them to sign off their annual assurance statements.

#### **4.4 Assessment of Risk**

- 4.4.1** When identifying risks, consideration needs to be given to external and internal drivers under the headings of financial, strategic, operational and hazard. This will help focus the risk assessment process.
- 4.4.2** When all the relevant risks have been identified a numerical scoring system is used to determine which are Key Risks to the Company's objectives. Risks are rated using two factors:
- **Likelihood** – An assessment is made of how likely the risk is to occur in practice; and
  - **Impact** – An assessment is made on if the risk did occur, what would be the impact on the Company.

Risks will be quantified in relation to their likelihood and impact in both financial and reputational terms

- 4.4.3** It is essential that the same principles for measuring risks are used across all Company activities so that risks can be compared across Services Areas and Directorates in a consistent manner. In order to ensure a consistent approach across NCH, specific criteria have been agreed for the likelihood and impact scores. These criteria are summarised in the table below:

<b>HOW TO MEASURE LIKELIHOOD (Vertical axis)</b>		
<b>LIKELIHOOD RATING</b>	<b>LIKELIHOOD DESCRIPTION</b>	<b>CRITERIA</b>
1 REMOTE	Virtually impossible	0 to 5% chance
2 UNLIKELY	Low but not impossible	6-20% chance
3 POSSIBLE	Fairly likely to occur	21-50% chance
4 LIKELY	More likely to occur than not	51-80% chance
5 ALMOST CERTAIN	Almost certain to occur	81% + chance

<b>HOW TO MEASURE IMPACT (Horizontal axis)</b>		
<b>IMPACT RATING</b>	<b>COST IMPACT</b>	<b>SCHEDULE IMPACT</b>
1 NONE	Negligible effect on projected cost (0-3%)	Negligible effect on projected schedule(<3%)
2 MINOR	Small increase (4-10%)	Small schedule slip (3-10%)
3 MODERATE	Significant increase (11–30%)	Significant slip (11-30%)
4 MAJOR	Large increase (31-75%)	Large delay (31-50%)
5 CATASTROPHIC	Major increase (>75%)	Major delay (>50%)

**4.4.4** Managers/RROs will decide on the likelihood and impact of each risk identified within their risk register. The Company's internal auditors may help to facilitate discussions, but managers are in a better position to be able to assess risks on the specific services their area(s) provide.

**4.4.5** The impact and likelihood of individual risks may change over time, therefore it is important to review the assessments which have been made on a regular basis.

#### **4.5 Risk Appetite**

- 4.5.1** A risk appetite or ‘tolerance’ will be established for each risk through identifying a risk score based on the individual ratings for risk ‘Impact’ and ‘Likelihood’ of occurrence i.e. performing a risk assessment.
- 4.5.2** The risk score can then be categorised into Low, Medium or High Risk which in turn triggers different levels of response. A 5x5 Risk Matrix will be used across the Company to measure risk.
- 4.5.3** Each risk is assessed for impact and likelihood before considering what controls are in place to manage it. The resulting score is called the ‘Inherent Risk Score’. The table below demonstrates the possible risk scores when the risk ratings are plotted on to the Risk Matrix:

<b>RISK MATRIX: KEY TO POSSIBLE RISK SCORES</b>						
		<b>IMPACT</b>				
<b>LIKELIHOOD</b>	<b>RATING</b>	1	2	3	4	5
	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

- 4.5.4** Depending upon the location of the risk score in the Risk Matrix, different actions are required. In general however, managers will identify what controls are already in place and ensure that existing and new adopted controls are operating effectively going forward. The table below summarises the specific actions required for the various risk score scenarios:

RISK SCORES	CONCLUSION AND ACTION REQUIRED
<b>1-4</b>	<p>Acceptable level of risk.</p> <p>No further action required to reduce risk, but managers should ensure that the relevant controls are operating effectively. Service Area Managers/RROs should also review the controls for low risk areas carefully, to ensure there are not too many controls in place.</p>
<b>5-11</b>	<p>Implementation of additional controls is required.</p> <p>The costs and benefits associated with implementing additional controls should be considered. The relevant Service Area Management Team may then agree that no further action should be taken. This decision must be recorded on the risk register.</p>
<b>12-25</b>	<p>Implementation of additional controls is required.</p> <p>Service Management Teams should identify, discuss, establish and implement additional systems, controls, processes and procedures designed to mitigate individual risks.</p> <p>If the Service Area Management Teams do not want to introduce any more controls or other measures to mitigate high level risks, they must seek approval from the Board. Any such agreement from the Board should be recorded on the risk register.</p>

**4.5.5** Service Managers/Risk Register Owners should perform a second risk assessment, rescoring each risk and document changes in their respective risk registers. Risk factors are generally reduced due to appropriate action being taken and as a result the re-calculated figure is called the residual risk score. As risk scoring can be a very subjective exercise, qualitative analysis of the key risks will be included in risk management reports.

**4.5.6** The level of risk will also impact upon the frequency of review and the level of monitoring. The table below outlines how and when risks, and the control established to mitigate them, should be monitored according to their respective risk scores.

<b>RISK SCORES</b>	<b>CATEGORY</b>	<b>MONITORED BY</b>	<b>FREQUENCY</b>
<b>1-4</b>	<b>Low (Green)</b>	Service Area Managers/Risk Register Owners and RM Panel.	Both Quarterly
<b>5-11</b>	<b>Medium (Amber)</b>	As above as well as Audit Committee and Executive Directors.	Bi-annually and Annually
<b>12-25</b>	<b>High (Red)</b>	As above as well as the Audit Committee and Company Board.	Quarterly and Annually

**4.5.7** At any one time the residual risk score of a number of individual risks may still be high, even after additional controls designed to reduce the level of risk have been implemented. Therefore, what constitutes an acceptable level of risk will be subject to discussion by the Audit Committee, on a quarterly basis, and ultimately annual approval by the Board.

## **4.6 Risk Management Activities**

**4.6.1** The Company undertakes a range of activities to manage, eliminate or control risks. In particular, it will:

- Annually review the Key Risks in conjunction with the Business Plan and Delivery Plan (Board)
- Review and update the Corporate and Service Area Risk Registers (Executive Management Team and Audit Committee);
- Scrutinise the risk registers and identify best practice (Risk Management Panel);
- Update the Corporate Risk Register to reflect risks associated with Corporate Plan objectives and high level risks identified within Directorates (Corporate Risk Officer).
- Annually report on the effectiveness of risk management and control (Director of Finance, ICT and Governance);
- Carry out risk assessments on all significant projects (Project Managers);
- Monitor the overall impact of new risks to ensure total risk levels remain within acceptable limits (Audit Committee);
- Report to Executive Management Team and monitor internal control failures and annually report on them to Audit Committee (Director of Finance, ICT and Governance);
- Require Directorate Leads to sign an annual certification of controls assurance (Executive Directors);
- Implement a programme of Risk Awareness Workshops and training to raise awareness of risk within the organisation (Director of Finance, ICT and Governance); and
- Focus Board papers on risk issues where appropriate (Executive Management Team).

## **4.7 Responsibilities**

**4.7.1** The Company has assigned responsibilities within the Risk Management Framework to ensure that risk activities and monitoring are carried out at the right level within the Company.

**4.7.2** The Director of Finance, ICT and Governance has been given responsibility for implementing the Risk Management Framework, but overall responsibility for the risk management system within the Company lies with the Chief Executive

**4.7.3** Responsibilities of the Board:

- To maintain an overview of the arrangements, make strategic management decisions and undertake top level monitoring;
- Approve the Risk Management Framework and ensure it is reviewed annually by the Audit Committee;
- Promote the desired mindset and attitude within the Company that is essential for robust risk management processes;
- Approve the risk targets and levels for each type of activity, seeking guidance from the Audit Committee where appropriate;
- Assess, monitor and review the Key Risks and the Corporate Risk Register on an annual basis; and
- Report to the City Council as required.

**4.7.4** Responsibilities of the Audit Committee:

- Review the Risk Management Framework annually and recommend changes to it;
- Recommend the Risk Management Framework to the Board;
- Recommend the total risk appetite;
- Report to the Board periodically;
- Recommend risk targets, limits and controls for different types of risk, referring higher level decisions to the Board;
- Assess, monitor and review the Key Risks and the Corporate Risk Register on a quarterly basis; and
- Assess, monitor and review the Directorate Risk Registers on a six monthly basis.

**4.7.5** Responsibilities of the Executive Directors / Executive Management Team:

- Prioritise risk levels in total and by type;
- Embed a culture of risk awareness in the Company;
- Complete annual control self assessment checklists that feed into the Company's overall internal control assurance statement;

- Approve and monitor the overall levels of risk in their service areas i.e. that established in their respective risk registers;
- Ensure that managers and RRROs are managing and controlling risks effectively and updating their risk registers on a timely basis; and
- The Director of Finance ICT and Governance will report quarterly to the Executive Management Team and the Audit Committee on risk management and annually to the Board on the risk management and the work of the Risk Management Panel.

**4.7.6** Responsibilities of Service Area Managers/Risk Register Owners (RROs), Risk Register Responsible Officers (RRROs) and Project Managers:

- Undertake major risk appraisals of operational areas through quarterly reviews;
- Implement the Risk Management Framework across all areas of responsibility;
- Manage and control risks;
- Ensure that risk registers are reviewed and updated on a timely basis together with the Service Area Management Teams;
- Ensure that significant high level risks are escalated to the Corporate Risk Register;
- Lead and encourage an appropriate culture for good risk management within and across areas of responsibility;
- Prepare proposals for initiatives, change programmes and developments using the methodology given within the Risk Management Framework or another risk based methodology; and
- Identify and ensure that adequate training is provided to service area staff where required.

**4.7.7** Responsibilities of the Risk Management Panel:

- Scrutinise all risk registers, including Service Area Risk Registers, before presentation to the Audit Committee, Executive Management Team or Board;
- Produce an annual risk update for the Board (to be incorporated into the report of the Director of Finance, ICT and Governance – see 4.3.20);
- Review the quarterly risk assessments to ensure robustness and completeness;
- Identify examples of best practice and promulgate these across the Company;
- Provide an internal training resource on risk management;
- Liaise with the relevant service areas over insurance and health & safety issues;

- Provide performance management information on risk management.

#### **4.7.8** Responsibilities of the Corporate Risk Officer (Company Secretary):

- Ensure that the Corporate Risk Register is reviewed and updated to reflect the risks associated with Delivery Plan objectives on an annual basis;
- Liaise with RRROs to ensure that significant high level service area and Directorate risks are included on the Corporate Risk Register, on a timely basis;
- Ensure that reporting and decision-making risks are included on the Corporate Risk Register where the associated report's risk assessment categorises them as high risk scores; and
- Liaise with the Head of Health and Safety to ensure that risks captured through safety audits, and considered to be high in terms of financial or reputational risk, are included in the Corporate Risk Register.

#### **4.7.9** Responsibilities of all Staff:

- Be aware of the risks associated with their work;
- Report any new risks to their line manager;
- Report any internal control failures to the Risk Management Panel; and
- Participate in annual reviews of departmental risks.

### **4.8 Other Reporting and Decision-making**

#### **4.8.1** There should be evidence to show that risks have been considered when key Company decisions are made, including:

- Reports to Board and Committees – all reports should include an assessment of the risks related to the subject and the course of action/recommendations proposed.
- Projects and Programme Initiatives – all projects should operate within the Prince 2 framework which requires that risks are acceptable before proceeding with initiation;
- Policy and Strategy Documents – all documents should be accompanied by a risk assessment in the covering report; and
- Key Executive Management Team (EMT) decisions – all key decisions should be supported by a risk assessment in the covering report.

#### **4.8.2** Reporting and decision-making risks should be included on the Corporate Risk Register where the associated risk assessment process categorises them as medium or high risk scores.

## **4.9 Partnerships**

**4.9.1** Where achievement of objectives relies on contributions from other internal or external stakeholders, responsibilities for management of risks should be agreed. It should be noted that where risks are managed by external stakeholders e.g. sub-contractors, any failure by them to adequately manage risk could have an impact on the reputation of NCH. Reputational risks will usually remain with the Company as such risks are difficult to transfer.

## **4.10 Health and Safety**

**4.10.1** Risks associated with Health and Safety should already be captured through safety audits and their associated risk assessments as well as implementation of the Health and Safety Strategy. However, to ensure that all risks are collated and reviewed as part of an integrated risk management process, such Health and Safety risks should be included in the H&S Service Area Risk Register and, ultimately, in the Corporate Risk Register where the impact of the risk is considered to be high in terms of financial or reputational risk.

## **4.11 Training, Job Descriptions and Performance Objectives**

**4.11.1** Training events will be provided for all managers to give them the necessary skills to carry out their own risk assessments and to produce and maintain risk registers (including identification and implementation of risk controls).

**4.11.2** Risk management roles and responsibilities should be added into individual job descriptions during the normal course of organisational review, especially where managers are assigned responsibility for their Service Area's Risk Register i.e. Risk Register Owners.

**4.11.3** Risk management should also be considered and assessed as part of the individual manager's Job Competencies and performance objectives, linking back to Job Descriptions. This would then ensure that risk management would be clearly part of NCH's performance management and assurance systems.

## **4.12 Performance**

**4.12.1** There are currently no BVPIs for risk management, although the Audit Commission has established best practice in the sector through their publication 'Worth the Risk' and recent Best Value reviews of risk management arrangements.

**4.12.2** NCH will continue to follow best practice in this area and has established the following local PIs:

- Reduce the number of reported control failures by 5% from the established base level;
- Reduce the number of claims made against the company's insurance policies by 5%;
- Reduce insurance costs by 5%; and
- Reduce the number of negative media stories (either in quantity or column inches) regarding the company by 10%.

**4.12.3** The successful completion of the corporate objectives will be the key indicator that NCH is managing its risks.

**4.12.4** NCH welcomes suggestions and comments from people who use or provide services to the organisation. NCH believes that this can provide some important lessons to help the company improve its services. Although there will be no formal tenant and leaseholder consultation on this framework, it will be regularly reviewed in light of good customer practice.

## 5. RISK MANAGEMENT ACTION PLAN

### 5.1 Risk Management Action Plan

5.1.1 The Risk Management Action Plan identifies the key tasks and milestones related to embedding risk management into the normal working activities of the Company as well as the associated critical success factors.

ISSUE	ACTION(S)	CRITICAL SUCCESS FACTOR	RESPONSIBLE OFFICER(S) & TARGET DATE
<p><b>Risk Management Framework and Strategy</b> Develop Risk Management Framework and Strategy for approval.</p>	<p>Draft, develop and approve the strategy and the actions recommended to ensure that risk management is embedded at all levels throughout the organisation.</p>	<p>Risk Management Framework is approved by the Company Board within the timescales agreed in the February 2008 Internal Audit Risk Management report.</p>	<p>Julie Crook (Director of Finance, ICT and Governance)  15<sup>th</sup> May 2008.</p>
<p><b>Risk Management Panel</b> Establishment of a Risk Management Panel with appropriate Terms of Reference.</p>	<p>Risk Management Panel chaired by the Company Secretary with nominated senior managers acting for each Executive Director of the Company. Terms of reference to include:</p> <ul style="list-style-type: none"> <li>• Ensuring corporate and other key risks are reported quarterly to the Board;</li> </ul>	<p>Establishment and 1<sup>st</sup> meeting of the Panel to be held to approve Terms of Reference and review risk registers.</p>	<p>Alison Mapp (Company Secretary)  31<sup>st</sup> May 2008.</p>

ISSUE	ACTION(S)	CRITICAL SUCCESS FACTOR	RESPONSIBLE OFFICER(s) & TARGET DATE
	<ul style="list-style-type: none"> <li>Production of an annual risk report.</li> </ul>		
<p><b>Risk Management Policy</b> Establishment of a Risk Management Policy included in the Members Handbook.</p>	<p>Included in the Risk Management Framework.</p> <p>RMF reviewed by the Audit Committee and approved by the Board annually, negating the need for the policy to be included in the Member's Handbook.</p>	<p>Risk Management Framework is approved by the Company Board within the timescales agreed in the February 2008 Internal Audit Risk Management report.</p>	<p>Julie Crook (Director of Finance, ICT and Governance)</p> <p>15<sup>th</sup> May 2008.</p>
<p><b>Corporate Risk Register</b> Draft Corporate Risk Register produced for review and approval.</p>	<p>Corporate Risk Register updated to reflect the high level risks (including ratings and mitigations) which could impact on NCH as a whole i.e. primarily the risks associated with the achievement of the Company's strategic objectives, set out in the Delivery Plan, as well as any significant high level risks included in Directorate Risk Registers.</p>	<p>Corporate Risk Register and the Key (Corporate) Risks that threaten business priorities reviewed and approved by Board.</p>	<p>Alison Mapp (Company Secretary)</p> <p>15<sup>th</sup> May (Board approval of CRR)</p> <p>18<sup>th</sup> Sept (Board approval of CRR – updated to reflect Directorate RRs).</p>
<p><b>Service Area Risk Registers</b> Draft Service Area Risk Registers produced for review and approval.</p>	<p>Appointed Service Area Managers/RROs review and update risk registers in line with the</p>	<p>Service Area Risk Registers are completed 3 weeks in advance of the June Audit</p>	<p>Service Area Managers/Risk Register Owners</p>

ISSUE	ACTION(S)	CRITICAL SUCCESS FACTOR	RESPONSIBLE OFFICER(s) & TARGET DATE
	requirements of the Risk Management Framework.	Committee.	(RROs) 16 <sup>th</sup> May 2008.
<b>Directorate Risk Registers</b> Draft Directorate Risk Registers produced for review and approval.	Appointed Risk Register Responsible Officers compile and review Directorate Risk Registers in line with the requirements of the Risk Management Framework.	Directorate Risk Registers are reviewed and approved by Audit Committee on a bi-annual basis.	Risk Register Responsible Officers (RRROs) 10 <sup>th</sup> June 2008.
<b>Corporate Risk Officer</b> Corporate Risk Officer to ensure identified risk management critical success factors are established and a plan of action is prepared and implemented.	Company Secretary assigned the role of Corporate Risk Officer.  Action plan included in the Risk Management Framework – reviewed annually.	Company Secretary appointed and assigned role of Corporate Risk Officer within the timescale agreed in the February 2008 Internal Audit Risk Management report.	Alison Mapp (Company Secretary)  31 <sup>st</sup> May 2008.
<b>Annual Risk Report</b> Develop and commence annual Board reporting on risk management.	Annual Board report by the Director of Finance, ICT and Governance on risk management, the Company's Key Risks and the work of the Risk Management Panel.	Report to accompany the Risk Management Framework and the Corporate Risk Register.	Julie Crook (Director of Finance, ICT and Governance)  15 <sup>th</sup> May 2008.
<b>Training and Education</b> Managers who have not been involved in producing risk registers, business plans,	Develop methods of improving awareness including briefings to	Completion of Service Area Risk Registers 3 weeks in	Service Area Managers/RROs

ISSUE	ACTION(S)	CRITICAL SUCCESS FACTOR	RESPONSIBLE OFFICER(S) & TARGET DATE
<p>project management documentation etc, may not have an understanding of risk management and may be unaware of how it impacts on their jobs.</p>	<p>teams and ad-hoc finance function support for lead managers/officers and teams trying to develop their own risk registers.</p> <p>Audit Committee risk management awareness training and appropriate training and guidance for all staff to enable them to take responsibility for managing risk within their own working environment.</p>	<p>advance of the June Audit Committee.</p> <p>Risk Management awareness training is provided to members within the timescales agreed in the February 2008 Internal Audit Risk Management report.</p>	<p>16<sup>th</sup> May 2008.</p> <p>Julie Crook (Director of Finance, ICT and Governance)</p> <p>10<sup>th</sup> June 2008.</p>
<p><b>Job Descriptions</b> Managers may not have an understanding of their responsibilities in relation to risk management and what tasks they need to undertake as part of their jobs.</p>	<p>Risk management roles and responsibilities should be added into individual job descriptions, especially where managers are assigned responsibility to maintain and monitor risk registers.</p>	<p>Job descriptions are updated to reflect the risk management responsibilities of the Corporate Risk Officer, Risk Register Owners and Responsible Officers in the new Company structure.</p>	<p>Martinette Proud (Interim Director of Organisational Development)</p> <p>30<sup>th</sup> September 2008</p>
<p><b>Individual Performance Objectives</b> Managers may not have an understanding of their responsibilities in relation to risk management, what tasks</p>	<p>Risk management should also be considered and assessed as part of the individual manager's Job</p>	<p>Action incorporated into the new NCH appraisal scheme for all staff with key risk</p>	<p>Executive Directors, Assistant Directors and</p>

ISSUE	ACTION(S)	CRITICAL SUCCESS FACTOR	RESPONSIBLE OFFICER(s) & TARGET DATE
they need to undertake as part of their jobs and how risk management links to NCH performance management and assurance systems.	Competencies and Performance Objectives, linking back to Job Descriptions.	management responsibilities.	Heads of Service 31 <sup>st</sup> March 2009.
<b>Project, Partnership and Contract Risk Management</b> Introduction of formal risk management into project management, partnerships and large contracts, aligned to the principles adopted for business risk management.	To be implemented and monitored through the work of the Risk Management Panel.	Key risks identified through the formalisation of risk management into project management, partnerships and large contracts are fed into the Corporate Risk Register.	Julie Crook (Director of Finance, ICT and Governance)  18 <sup>th</sup> September 2008.

## 6. APPENDICIES

### 6.1 Appendix A - Terms and Definitions

6.1.1 It is important that all staff speak the same risk language. To this end NCH has defined the following terminology in line with the IRM Risk Management Standard;

- **Risk:** combination of the **probability** of an **event** and its **consequence**. The term **risk** is generally used only when there is at least the possibility of negative **consequences**. In some situations, **risk** arises from the possibility of deviation from the expected outcome or **event**.
- **Consequence:** outcome of an **event**. There may be more than one consequence from an event. Consequences can range from positive to negative and can be expressed qualitatively and quantitatively.
- **Probability:** extent to which an **event** is likely to occur. Degrees of belief about probability can be chosen as ranks, such as rare/unlikely/moderate/likely/almost certain.
- **Event:** occurrence of a particular set of circumstances. The event can be certain or uncertain, with a single occurrence or a series of occurrences. The **probability** associated with the event can be estimated for a given period of time.
- **Source:** item or activity having a potential for a **consequence**.
- **Risk criteria:** terms of reference by which the significance of **risk** is assessed. Risk criteria can include cost-benefit, legal requirements, environmental aspects or concerns of stakeholders.
- **Risk assessment:** The overall process of assessing the **impact** of a **risk** and the **likelihood** of its occurrence i.e. process of **risk analysis** and **risk evaluation**
- **Risk analysis:** systematic use of information to identify **sources** and to estimate the **risk**.
- **Risk identification:** process to find, list and characterise elements of **risk**.
- **Risk estimation:** process used to assign values to the **probability** and **consequences** of a **risk**.
- **Risk evaluation:** process of comparing the estimated **risk** against given **risk criteria** to determine the significance of the **risk**.
- **Risk treatment:** process of selection and implementation of measures to modify **risk**. Risk treatment measures can include avoiding, optimising, transferring or retaining **risk**.

- **Risk control:** actions implementing **risk management** decisions. Risk control may involve monitoring, re-evaluation and compliance with decisions.
- **Risk optimisation:** process, related to a **risk**, to minimise the negative and maximise the positive **consequences** and their respective **probabilities**.
- **Risk reduction (mitigation):** actions taken to lessen the **probability**, negative **consequences** or both, associated with a **risk**, through specific controls.
- **Mitigation:** limitation of any negative **consequence** of a particular **event**.
- **Risk avoidance:** decision not to become involved in, or action to withdraw from, a **risk** situation.
- **Risk transfer:** sharing with another party the burden of loss or benefit from gain, for a **risk**. Risk transfer can create new **risks** or modify existing **risk**.
- **Risk retention:** acceptance of the burden of loss, or benefit of gain, from a particular **risk**. Risk retention includes the acceptance of **risks** that have not been identified.
- **Risk acceptance:** decision to accept a **risk**.
- **Residual risk:** the **exposure** arising from a specific **risk** after action has been taken to manage it (making the assumption that the action has been effective) i.e. **risk** remaining after **risk treatment**. Residual risk should be lower than the **inherent risk**.

**6.1.2** Summarised below are a number of other useful definitions of risk management terminology;

- **Risk management:** the process of controlling **risks** to ensure that they are reduced to an acceptable level.
- **Risk rating:** derived from the scoring mechanism and designed to allow the organisation to prioritise its **Risk management** activities.
- **Risk score:** each risk is assessed for **impact** and **likelihood** before considering what **controls** are in place to manage it. The resulting score is called the '**Inherent Risk Score**' and is derived as the factor of the individual **risk impact** and **likelihood** risk ratings.
- **Risk Matrix:** the mechanism used to display the **risk scores** produced as a result of the various **risk ratings**.
- **Risk profile:** the documented and prioritised overall assessment of the range of specific **risks** faced by the organisation.

- **Risk response:** actions taken to mitigate a **risk**.
- **Inherent (Gross) risk:** the **exposure** arising from a **risk** before any action has been taken to manage it. Recurrent **risks** that arise through an organisations existence in an environment i.e. not necessarily through its actions or choices, are often referred to as inherent risks.
- **Assurance:** an evaluated opinion, based on evidence gained from review, on an organisation's governance, **Risk Management** and internal control framework.
- **Exposure:** the **consequences** (as a combination of impact and likelihood) which may be experienced by an organisation if a specific **risk** is realised.
- **Likelihood** – an assessment is made of how likely the risk is to occur in practice.
- **Impact** – an assessment is made on if the risk did occur, what would be the impact on the Company.

## **6.2. Appendix B - Key Objectives of Nottingham City Homes**

### **6.2.1** The key objectives are:

- Objective: To value the diversity of our customers and ensure our services are accessible to all;
- Objective: To involve, listen and be accountable to our customers;
- Objective: To achieve excellent housing services (and 2 stars in November 2008);
- Objective: To achieve and maintain decent homes;
- Objective: To be a key partner in transforming and managing Nottingham's neighbourhoods;
- Objective: To respond to the needs of the most vulnerable and socially excluded; and
- Objective: To be an excellent, efficient organisation which has high quality leadership and management and delivers value for money.

### **6.2.2** Our Mission and Vision are is “To deliver excellent services” and to have “Homes and places people want to live”.

### **6.2.3** Our values are:

- Tell the Truth;
- Keep Your Promises;
- Be Fair;
- Respect the Individual;
- Work as One Team;
- Encourage Fresh Thinking; and
- Strive for The Best.

### 6.3 Appendix C - Risk Management Cycle

6.3.1 The Risk Management cycle sets out an annual process for completing the Risk Management Framework. It details the activities that should be followed at each stage.

STEP	ACTIVITY
<p><b>1) IDENTIFICATION</b></p> <p>Identify what are the critical risks to achieving objectives.</p>	<p>Consider the use of workshops, checklists (available on the NCH intranet), Questionnaires, Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis, Analysis of the Political, Economic, Social, Technological, Legal and Environmental (PESTLE) factors, use real data from incident reporting and other systems to see what has occurred.</p> <p>It is also helpful to categorise risks at this stage for the purposes of this framework, the categories identified by the Office of Government Commerce (2004) will be used. These are:</p> <ul style="list-style-type: none"> <li>• <b>Strategic risks</b> - Linked to the Corporate Plan;</li> <li>• <b>Project/programme risks</b> - Specific projects and programmes ; and</li> <li>• <b>Operational risks</b> - Specific to service areas.</li> </ul> <p>The checklists under these categories are available on the intranet. Absolute accuracy and consistency is not essential as this is just a way of grouping similar risks for monitoring and reporting purposes. There is no specific section on partnership risks but the project/programme list can be used as a proxy for this. All risks on each risk register should be categorised.</p>

STEP	ACTIVITY
<p><b>2) OWNERSHIP</b></p> <p>Establish who is responsible for managing the risk.</p>	<p>All risks must be assigned an owner.</p> <p>The owner means the person who must understand, monitor and control the risk but does not have to be the one that directly takes all actions to mitigate a particular risk. It is important that the owner is involved in determining a risk score. Risk owners must have sufficient authority to take on responsibility for their risks.</p>
<p><b>3) ANALYSIS</b></p> <p>Measure the risks identified to determine a risk score.</p>	<p>Score the risks identified using the 5x5 matrix set out in the risk measurement section.</p> <p>This stage should rank risks in order of importance.</p>
<p><b>4) TOLERANCE “APPETITE”</b></p> <p>The level of risk we are prepared to accept to achieve our objective.</p>	<p>The risk appetite is the level at which a risk is deemed acceptable with or without any controls being applied. Setting target risk levels should also drive both action and exception reporting so that only risks that are outside of tolerable levels are escalated.</p> <p>Set a Target Risk Score.</p>
<p><b>5) RESPONSES</b></p> <p>Identify what controls will be used to mitigate the risk.</p>	<p>Consider and agree which approach(es) are most appropriate to meet target risk score:</p> <ul style="list-style-type: none"> <li>• Terminate: stop the activity that is producing the risk;</li> <li>• Prevention: prevent the risk having an impact;</li> <li>• Tolerate: accept the risk because its impact and likelihood are low and/or other control options are unacceptable because of e.g. cost;</li> <li>• Transfer: move the risk to another organisation e.g. through insurance. Note that it is difficult to transfer reputational risk; and</li> <li>• Take the risk which relates to taking opportunities rather than doing nothing.</li> </ul> <p>It is important to quantify in financial terms the actual or estimated costs of implementing</p>

STEP	ACTIVITY
	<p>the responses. Risk responses need to be proportionate to the risks involved.</p> <p>Prepare contingency plan to mitigate risk.</p>
<p><b>6) IMPLEMENT RESPONSES</b></p> <p>Implement the controls identified.</p>	<p>Implement the most appropriate response to the risk.</p> <p>This should be based on seeking to reduce the risk and moving it to within acceptable tolerances as defined previously.</p> <p>Actions should be incorporated into routine plans, projects plans etc rather than be maintained as separate risk action plans.</p> <p>Prior to implementation, there should be clarity as to how the effectiveness of a particular action is going to be measured.</p>
<p><b>7) GAIN ASSURANCE ABOUT RESPONSES</b></p> <p>Obtain evidence about the effectiveness of the control(s).</p>	<p>It is incorrect to assume that every control chosen and implemented is the correct one and has the effect of reducing a risk. In some cases, this will happen. In others, the control will have negligible impact and rarely, a control could increase the risk rather than, as intended, to reduce it.</p> <p>Apply the measurement previously determined after the control has been implemented. Has it had the desired effect or not? Is the risk within set tolerance levels?</p>

STEP	ACTIVITY
<b>8) COMPLETE SCORING OF RESIDUAL RISK RATINGS</b>	<p>Rate the risks again using the same 5x5 matrices.</p> <p>Have the scores changed? Has the risk changed category?</p> <p>If no change or a deterioration, need to go back to step 5 to determine different and more appropriate controls to achieve target risk score.</p>
<b>9) REPORTING</b>	<p>Formally report on risks to relevant body (Risk Management Panel, Executive Management Team, Audit Committee) together with controls to mitigate risks and an assessment of their effectiveness. This can be done on a comprehensive basis (all risks), selective basis (only high risks), or categorical basis (strategic risks) depending on the requirements of the particular forum. Agree the frequency of risk reports in the relevant forums.</p>
<b>10) REVIEW</b>	<p>Review how effective the Risk Management Cycle has been overall, including:</p> <ul style="list-style-type: none"> <li>• Has the process added value?</li> <li>• Has there been a positive outcome?</li> <li>• What evidence exists to demonstrate this?</li> <li>• How does this get communicated and to whom?</li> <li>• Were the reporting processes appropriate and reports well received?</li> <li>• What should be done differently next time?</li> </ul>

## 6.4 Appendix D - Risk Register Evaluation Form

6.4.1 The Risk Register Evaluation Form should be used by Service Area Managers/RROs and Executive Directors to evaluate the content of their risk registers against the NCH Risk Management Framework.

<b>Service Area:</b>
<b>Service Director:</b>

- 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 rating and resulting scores are reasonable and within tolerable limits**  
(Poor) 1 2 3 4 5 6 7 8 9 10 (Excellent)

## **6.5 Appendix E - Risk Checklist**

**6.5.1** To analyse impact and probability individuals need to consider both the threats (sources) and effects of risk. One threat may give rise to several effects, and there may be several threats which result in any particular effect. In addition, a 'domino effect' is highly probable; this is when the impact of one risk becomes the threat of further risk(s). Each of these subsequent threats needs to be analysed, and appropriate responses considered.

**6.5.2** When identifying risk individuals should think in terms of the following (or similar) phrases to express the risk in terms of threat and impact (or cause and effect):

- There is a risk of/that (...) which may result in (...); or
- There is a threat of (...) which may result in (...).

**6.5.3** Most risk will have the potential to lead to a detrimental effect on costs, timescales or the quality of the outcome (here operational concerns should be considered and addressed by the project if appropriate). By concentrating on the threats individuals and organisations are most likely to be able to take action that will reduce the impact.

**6.5.4** There are a large number of prompt lists available to help organisations categorise risk and these should be adapted to individual circumstances. Paragraphs 6.5.5 to 6.5.13 below provide key risk prompts that should be used by Members, Executive Directors and Service Area Managers/RROs when establishing areas of most concern and the associated risks.

### **STRATEGIC RISK – MAJOR THREATS**

**6.5.5** Sources of threat that may give rise to significant strategic risks include:

- Budgeting - relates to availability and/or allocation of resources;
- Unethical dealings;
- Product and/or service failure - resulting in lack of support to business processes;
- Public perception and reputation;
- Lack of business focus;
- Exploitation of workers and/or suppliers - availability and retention of suitable staff;
- Occupational health and safety mismanagement and/or liability;
- Failure to comply with legal and regulatory obligations and/or contractual aspect - can you sue or be sued?;
- Civil action;

- Failure of the infrastructure - including utility supply systems, computer networks, etc;
- Failure to address economic factors - such as interest rates, inflation;
- Political and market factors - e.g. for management of risk, security, etc;
- Operational procedures – adequate and appropriate;
- Information/communication – adequate and appropriate;
- Capacity to innovate and/or to exploit opportunities;
- Failure to control intellectual property;
- Failure to take account of widespread disease or illness among the workforce;
- Failure to complete to published deadlines or timescales;
- Failure to take on new technology where appropriate to achieve objectives;
- Failure to invest appropriately;
- Failure to control IT effectively;
- Failure to establish a positive culture following business change;
- Vulnerability of resources – materials, equipment and people;
- Failure to establish effective contingency arrangements in the event of a product and/or service failure;
- Failure to establish effective continuity arrangements in the event of a disaster;
- Environmental (mis)management - issues relating to fuel consumption, pollution, etc;
- Inadequate insurance/contingency provision; and
- Disasters such as fire, flood, building subsidence, bomb incident.

## **THREATS TO PROJECTS OR PROGRAMMES**

The categories below can be used as a starting point for identifying the main areas of risk in relation to NCH's projects or programmes.

### **6.5.6 Corporate and Commercial Risks.**

- Underperformance to specification.
- Management's underperformance against expectations.
- Contractors go out of business.
- Failure of suppliers to meet contractual requirements; this could be in terms of quality, quantity, timescales or their own exposure to risk.
- Insufficient capital revenues.
- Market fluctuations.
- Fraud/theft.
- Partnerships failing to deliver the desired outcome.

- The situation being non-insurable or cost of insurance outweighing the benefit the cover provides.
- Lack of availability of capital investment.

#### **6.5.7** Financial, Economical and Market Risks.

- Interest rate instability.
- Inflation.
- Shortage of working capital.
- Failure to meet projected revenue targets.
- Market developments will adversely affect plans.

#### **6.5.8** Legal and Regulatory Risks.

- New or changed legislation may invalidate assumptions upon which the activity is based.
- Failure to obtain appropriate approval, such as planning consent.
- Unforeseen inclusion of contingent liabilities.
- Failure to achieve satisfactory contractual arrangements.
- Unexpected regulatory controls or licensing requirements.
- Changes in tax structure.
- Infringement of personal data protection criteria.

#### **6.5.9** Organisational Management and Human Factors.

- Management incompetence.
- Inadequate corporate policies.
- Inadequate adoption of management practices.
- Poor leadership.
- Key personnel who have inadequate authority to fulfil their roles.
- Poor staff selection procedures.
- Lack of clarity over roles and responsibilities.
- Vested interests creating conflict and compromising the overall aims.
- Individual or group interests will be given unwarranted priority
- Personality clashes.
- Indecision or inappropriate decision making.
- Inadequate management of expectations.
- Lack of operational support.
- Inadequate or inaccurate information.
- Health and safety compromised e.g. physical dangers at work or prolonged staff stress.

#### **6.5.10** Political and Social Factors.

- Change of government policy - national or international.
- Change of government.

- Adverse public opinion/media intervention.

#### **6.5.11 Environmental Factors.**

- Natural disasters.
- Storms, floods, etc.
- Pollution incidents.
- Transport problems, including aircraft/vehicle collisions.

#### **6.5.12 Technical, Operational and Infrastructure Risks.**

- Inadequate design.
- Professional negligence.
- Human error/incompetence.
- Infrastructure failure.
- Operational lifetime shorter than expected.
- Residual value of assets lower than expected.
- Increased dismantling/decommissioning costs.
- Safety being compromised.
- Performance failure - people or equipment.
- Residual maintenance problems.
- Unclear expectations/objectives.
- Breaches in physical security/information security.
- Lack or inadequacy of business continuity and contingency measures with regard to this activity.
- Unforeseen barriers or constraints due to infrastructure.

### **OPERATIONAL RISKS**

#### **6.5.13 Aspects to cover here include:**

- Lack of clarity of service requirements;
- Inadequate infrastructure to provide required operational services;
- Inadequate or inappropriate people available to support the required service provision;
- Inappropriate contract in place and/or inadequate contract management to support required level of service provision;
- Changing requirements, enabled in an uncontrolled way;
- Products passed to operational teams without due consideration to implementation, handover, subsequent maintenance and decommissioning;
- Unexpected or inappropriate expectations of service users;
- Inadequate incident handling;
- Lack or inadequacy of business continuity or contingency measures with regard to maintaining (critical) business services;

- Lack of investment in infrastructure to support future needs/opportunities; and
- Failing to meet legal or contractual obligations.

**Source**

**Management of Risk: Guidance for Practitioners  
Office of Government Commerce, (HMSO) 2004**