
# Risk Management Policy and Framework

## March 2018
## Version 1.04
**(Update for Governance, Risk and Audit Committee – March 2018)**

# Foreword

The fundamental principles adopted by the Council on Risk Management are described within the policy statement on Risk Management.

Adopting and implementing the strategy detailed below will achieve compliance with the policy.

Internal audit have just completed the Assurance Review of Risk Management, the objective of the audit was to review the systems and controls in place within Risk Management, to ensure they are operating adequately, effectively and efficiently.

The audit concluded that the systems and processes of internal control are deemed 'Substantial' in managing the risks associated with the audit. The previous report on Risk Management (NN/16/03) was issued in November 2015 and concluded in a ‘Reasonable’ assurance opinion. This indicates a positive direction of travel and that the system of controls has improved since the previous audit.

# Contents

## Policy Statement

This policy will take effect from the date of approval (Governance, Risk and Audit Committee). It is the policy of the Council to adopt a proactive approach, through its management processes, to risk management of the services it delivers both for itself and in partnership with others.

It is recognised that a certain amount of risk is necessary and indeed that it can be a positive force in the development of the services we provide. However, this needs to be managed in order to:-

- Safeguard our clients or service users, Members and employees and all other persons to whom the Council has a duty of care
- Ensure compliance with statutory obligations
- Preserve and enhance service delivery
- Protect our property, including buildings, equipment, vehicles and all other assets and resources
- Maintain effective control of public funds
- Protect and promote the reputation of the Council
- Support the quality of the environment
- Achieve the objectives in the Corporate Plan and Service Plans
- Safeguard the information we hold, obtain, record use and share based on the new General Data Protection Regulations (GDPR)

All of these objectives will be achieved by applying the Council's risk management strategy, which outlines responsibilities for managing risks and defines how risk management should be applied across the Council.

The master copy of this document, a record of review and decision making processes will be held by the Head of Finance and Assets. All documentation will be available for audit as necessary.

This policy will be available to all staff and Members on the corporate document register on the intranet.

## 2. Strategy Background

All organisations face a wide variety of risks including physical risks to people or property, financial loss, failure of service delivery, information management and damage to the organisation's reputation. Risk for this purpose is defined as "the chance of an event happening and leading to unintended effects which will impair

the organisation's ability to achieve its objectives".

Risk management is intended to be a planned and systematic approach to the identification, assessment and management of the risks facing the organisation.

The traditional means of protecting against the more obvious risks has been through insurance. However, there are many risks which cannot be insured against and which must be addressed in different ways. Even in the case of those risks which are insurable, action can be taken to reduce the potential risks with consequent savings of premiums and disruption of work.

The risk management strategy aims to:-

- Clarify responsibilities for identifying and managing risks
- Ensure that an appropriate level of risk management is consistently applied across the Council
- Increase awareness and use of risk management as a normal element of service management and improvement
- Facilitate sharing of experience and good practice across the Council and with other bodies

## 3. Leadership and Responsibility

Given the diversity of Council services and the wide range of potential risks, it is essential that responsibility for identifying and taking action to address potential risks is clear.

Responsibility for effective risk management rests with all Members and Officers of the Council.

The Corporate Directors and Heads of Paid Service are the Officers with overall responsibility for securing adherence to the Council's policy on Risk Management. Nick Baker is also designated as the Council's Senior Risk Information Officer (SIRO) and will take overall ownership of the Council's Information Risk Policy, act as champion for information risk on the Corporate Leadership Team and provide written advice to the Head of Finance and Assets on the content of the Council's Statement of Internal Control in regard to information risk.

The framework of roles and responsibilities in Appendix One shows how these are allocated.

## 4. Corporate Governance

North Norfolk District Council has adopted a Local Code of Corporate Governance setting out the framework through which it will carry out its responsibilities to deliver effective services.

Core principle four requires “taking informed and transparent decisions which are subject to effective scrutiny and managing risk”. This requires that an effective risk management system is in place.

As part of the Local Code it states that the authority should prepare and publish an Annual Governance Statement (AGS). This statement is a key corporate document and will include an assessment of the authority’s effectiveness of managing risk; it is signed by the Corporate Directors and Heads of Paid Service and Leader of the Council.

The assessment of the authority’s effectiveness of managing risk is provided by an annual report to the Governance, Risk and Audit Committee.

To enable links to be made to the Corporate Plan the Corporate Risk Register identifies the Corporate Objective / Service priority to which that risk is identified.

## 5. Resourcing Risk Management

Risk management is not a new issue and, as identified in the Leadership and Responsibility Section, every Member and Officer is responsible for considering risk implications as they relate to their actions. Since the adoption and implementation of the Risk Management Framework in 2010 the concept of risk management has been formalised and is part and parcel of the culture of the Council.

The designated Risk Champion(s) at Management Team Level is the Head of Finance and Assets who also covers the role of Corporate Risk Officer.

Information Technology is used in the form of the Performance and Risk System.

## 6. Role and Composition of the Risk Management Board

Whilst acknowledging the wide variety of risks that face the Council, and the differing circumstances that apply in different services, it is essential that there is some consistency in the way that risks are identified and assessed. This helps to ensure that all areas of risk are adequately considered and relative priorities for action can be judged.

The Risk Management Board will provide this consistency of approach. The Board acts as a link between service managers, specialised groups dealing with particular areas of risk, senior management and Members.

The Board consists of the Leader and Deputy Leader of the Council and the Portfolio Holder for Finance, all the Corporate Leadership Team, The Head of Finance and Assets and the HR Manager.

The Terms of Reference and membership of the Risk Management Board are available on the Intranet.

The Corporate Risk Register will be a standing item on the agenda (for any issues or changes that arise) and a full review of the register will take place every six months.

## 7. Risk Management Role in the Cabinet and Governance, Risk and Audit Committee

The Cabinet is responsible for ensuring that an adequate risk management framework and associated control environment exists within the Council.

The Audit Committee was established in 2006 but has now been replaced by the Governance, Risk and Audit Committee. This Committee is responsible for monitoring the arrangements in place for the identification, monitoring and management of strategic and operational risk.

To provide the Governance, Risk and Audit Committee with the necessary information to undertake these responsibilities, regular progress updates on the Corporate Risk Register are reported at specific meetings.

## 8. Risk Management Approach

The development of a consistent, corporate approach to risk management is done in a methodical and proportionate way in order to avoid the creation of a self-defeating bureaucratic burden.

To ensure that risk management is handled in the most efficient way within the Council, the risk element has been included in the Service Plans and the work to implement the risk management strategy has been included in the Performance and Risk System.

## 9. Methodology

A methodology for identifying, assessing and managing risk within the Council has been developed. This methodology has the advantage of being relatively straightforward to use and can be applied to both the strategic risks of the Council and as part of the routine service and project planning processes.

Guidance for managers on the application of the risk management methodology has been produced and is embedded in the Performance and Risk System. Risk review meetings between the Policy and Performance Management Officer and Service Managers are held at least every six months to review and updated the assessment of existing risk and their management, to identify new risks and risks that should be put forward for inclusion in the Corporate Risk Register.

Risk assessments should be produced to support strategic policy decisions and all major projects. The Guide to Project Management (on the Intranet) includes how to assess risk and has forms to capture the data. The Council's risk management

methodology should be followed to produce these risk assessments and a summary of the findings given in reports to Members.

Risk management training will be provided for managers to assist with implementing the risk management methodology. Managing Risk is a tutorial in the e-learning portal.

# 10. Risk Scoring, Matrix and Risk Tolerance

## Corporate Risks

Each corporate risk (a similar matrix is used for service risks) will be assessed against the following criteria:

| Corporate Risk | | | | | |
|---|---|---|---|---|---|
| **Impact Type** | **Catastrophic 5** | **Critical 4** | **Moderate 3** | **Marginal 2** | **Negligible 1** |
| **Objectives** | The key objectives in the Corporate Plan will not be achieved. | One or more Key Objectives in the Corporate Plan will not be achieved. | Significant impact on the success of the Corporate Plan. | Some impact on more than one Service. | Insignificant impact on more than one Service. |
| **Financial Impact (Loss)** | Over £1.5m | £500K - £1.5m | £300K - £500K | £0K - £300K | £0-20K |

Likelihood ratings and dimensions are tabled below

| Grade | Likelihood | Probability | Timing |
|---|---|---|---|
| 5 | Very High | Over 90% | Within six months |
| 4 | High | 60 - 90% | This year |
| 3 | Moderate | 40 - 60% | Next year |
| 2 | Low | 10 - 40% | Probably within 15 years |
| 1 | Very Low | below 10% | Probably over 15 years |

## Instructions issued with service plans

Impact ratings and dimensions are tabled below.

| Corporate Risk | | | | | |
|---|---|---|---|---|---|
| **Impact Type** | **Catastrophic 5** | **Critical 4** | **Moderate 3** | **Marginal 2** | **Negligible 1** |
| **Objectives** | The key objectives in the Corporate Plan will not be achieved. | One or more Key Objectives in the Corporate Plan will not be achieved. | Significant impact on the success of the Corporate Plan. | Some impact on more than one Service. | Insignificant impact on more than one Service. |
| **Financial Impact (Loss)** | Over £1.5m | £500K - £1.5m | £300K - £500K | £20K - £300K | £0-20K |

| Service Risk | | | | | |
|---|---|---|---|---|---|
| **Impact Type** | **Catastrophic 5** | **Critical 4** | **Moderate 3** | **Marginal 2** | **Negligible 1** |
| **Objectives** | The key objectives in the Business Plan will not be achieved | One or more Key Objectives in the Business Plan will not be achieved. | Significant impact on the success of the Service Business Plan. | Personal or team objectives not met. | Insignificant impact. |
| **Financial Impact (Loss)*** | Over £500K | £300K - £500K | £75K - £300K | £10K - £75K | £0-10K |
| **Service provision** | Service suspended long term or statutory duties not delivered. | Service suspended short term. | Service reduced significantly | Slightly reduced | No effect |

* Note: these are indicative figures it may be better to use % of budget for some of the smaller services.

Likelihood ratings and dimensions are tabled below

| Grade | Likelihood | Probability | Timing |
|---|---|---|---|
| 5 | Very High | Over 90% | Within six months |
| 4 | High | 60 - 90% | This year |
| 3 | Moderate | 40 - 60% | Next year |
| 2 | Low | 10 - 40% | Probably within 15 years |
| 1 | Very Low | below 10% | Probably over 15 years |

The probability and timing are guidelines only and should be used with judgement. For example: an identified risk happened in the last six months but had not occurred previously for over 10 years. The likelihood of it happening again is still probably still Low, particularly if you feel that any new controls put in place since the risk happened have made it less likely.

## Risk Matrix

The scoring by using a 5x5 matrix, which multiplies the numbers together, gives a wider range of scores.

**Matrix**

| Likelihood of occurrence | | | | | | |
|---|---|---|---|---|---|---|
| | **5** | 5 | 10 | 15 | 20 | 25 |
| | **4** | 4 | 8 | 12 | 16 | 20 |
| | **3** | 3 | 6 | 9 | 12 | 15 |
| | **2** | 2 | 4 | 6 | 8 | 10 |
| | **1** | 1 | 2 | 3 | 4 | 5 |
| | **Multiply** | **1** | **2** | **3** | **4** | **5** |

### *Severity of impact / consequences*

A very high likelihood with a catastrophic impact would score 25 but something that was very low likelihood and negligible impact would only score 1.

## Risk Tolerance

**Matrix**

| Likelihood of occurrence | | | | | | |
|---|---|---|---|---|---|---|
| | **5** | 5 | 10 | 15 | 20 | 25 |
| | **4** | 4 | 8 | 12 | 16 | 20 |
| | **3** | 3 | 6 | 9 | 12 | 15 |
| | **2** | 2 | 4 | 6 | 8 | 10 |
| | **1** | 1 | 2 | 3 | 4 | 5 |
| | **Multiply** | **1** | **2** | **3** | **4** | **5** |

### *Severity of impact / consequences*

A score of 6 or under is deemed marginal and requires no further action
A score of between 7 and 14 is deemed moderate and requires action to reduce the score.
A score of over 15 is deemed critical and requires immediate action.

# 11. Risk Identification

To meet the requirements of this framework, risk(s) must be capable of being identified at any level, and by anybody, within the Authority.

The key people are the service managers who will be actively monitoring their service plan to identify risks and change management practices and controls to

reduce their impact. They can also be escalated to being a corporate risk through the Risk Management Board, as can Members.

## 12. Risk Registers

The authority has three levels of risk register. The Corporate Risk Register which is maintained by the Corporate Risk Officer (Head of Finance and Assets) and monitored by the Risk Management Board. The service risks are monitored through the service plans and recorded on the TEN system. There are also individual risk registers for certain projects such as the waste and leisure procurements and the new leisure schemes which include the re-provision of leisure facilities in Sheringham and the new Cromer Sports Hub. Reviewing service risks is the responsibility of the service manager with the support of the Policy and Performance Management Officer.

There is no "classic" definition of corporate risk as each organisation is different, however, as a guide a risk that would be described as corporate is one that would adversely affect the delivery of the corporate plan or mean the failure to deliver a corporate objective or affects more than one area of operation.

The Corporate Risk Register is in the following format:

| **Name/No**<br><br>1. Cause of risk<br><br>2. Description of Risk or potential event<br><br>3. Consequence of risk happening | **Existing Controls** | **Score (with controls)**<br><br>Impact x Likelihood = Total | **Action** (to achieve target score) and Date for action to be completed | **Target Score**<br><br>Impact x Likelihood = Total | **Corporate Objective / Service Priority** | **Responsi-ble Officer** |
|---|---|---|---|---|---|---|
| | | | | | | |

The method of scoring likelihood and impact is in section 10.

Similarly there is no "classic" definition of service risk and it is the clear intention to only collect and monitor the main risks that face a service. In a similar way to the corporate risk, a service risk is one that would adversely affect the delivery of the services business plan or mean the failure to deliver a service objective or affects more than one area within the service.

The service risks are gathered in a similar way:

| Ref | **Description of risk/ opportunity factor**<br><br>1. Cause of risk<br><br>2. Description of risk<br><br>3. Consequence of risk occurring | **Existing controls** in place to reduce the risk. | **Risk Score** | | **Action** to reduce risk score with timescale and responsible officer | **Target Score** | | **Affected Corporate Objective or Service Activity** |
|---|---|---|---|---|---|---|---|---|
| | | | I | L | | I | L | |

All service plans will have the risk element completed and signed off by the relevant Head of Service. For each risk the category or categories of risk are identified to assist in assessing the kind of control, mitigation and contingencies that should be put in place.

Categories of risk;

A Financial
B Reputational
C Capacity/Delivery?
D Statutory Compliance
E Human Resources
F Partnership
G Health and Safety

The TEN Performance system will show risks by service and risks and controls must be reviewed on a regular basis, the framework requires a six monthly update which will be facilitated by the Policy and Performance Management Officer.

## 13. Involvement of Other Related Groups

There are a number of other officer groups in existence which deal with specific areas of risk management. These include both the Health and Safety Group and the Corporate Business (Service) Continuity Group. These groups are represented on the Risk Management Board by their Corporate Directors so that their work can be coordinated with the overall management of the risks facing the Council.

In addition to the groups listed above, the Council's Internal Audit section also contributes to the management of risk. The work of Internal Audit is based on a needs and risk assessment process that identifies and focuses resources on higher risk areas. Audit findings are reported to the relevant Chief Officer and Service Manager together with recommendations for improvement and an action plan. Checks are undertaken by Internal Audit to ensure agreed recommendations are implemented.

The Corporate Risk Officer will receive copies of all finalised internal and external audit reports to assess if any change is required for the risk registers.

## 14. External Contacts

The potential risks faced by the Council are in many cases similar to those faced by other authorities and it is practical and cost effective to learn from the experience of others.

In order to share risk management information and experiences, the Council has established networks with other authorities and agencies. Specifically, the Council is a member of the Norfolk Risk Managers' Group. This Group, whose members include local authorities, police authority and others from Norfolk, meets on a

regular basis to discuss risk management issues that are common to organisations and to share examples of best practice.

## 15. Linked Policies

There are a number of policies that are or will be linked to this framework:

- Health and Safety Policy
- Information Management Strategy
- Information Risk Policy
- IT Security Policy
- Business Continuity Policy

## 16. Review Process

**This Framework will be reviewed by the Corporate Risk Board and any amendments will be agreed by the Governance, Risk and Audit Committee.**

# Appendix 1: Shared Leadership – Role and Responsibilities

Everyone has a role to play in an integrated risk management framework. Combining shared leadership with a team approach will help contribute to its ultimate success. Roles as identified at present are:

1. FULL COUNCIL

Approve the Corporate Risk Management Framework which includes the Policy Statement and Strategy.

2. CABINET

To provide leadership and direction for the Council. To keep the Council's policies and objectives under review, including the Council's corporate strategic risks, and agree a programme of risk reduction where appropriate.

Receive progress reports on risk reduction programme and agree revisions to "corporate risk register".

Assess risks attached to proposals for new / changed policies and service delivery arrangements and make recommendations to Full Council.

3. GOVERNANCE, RISK AND AUDIT COMMITTEE

Monitor to ensure that an adequate risk management framework and associated control environment is in place.

Monitor arrangements for the identification, monitoring and management of strategic and operational risk within the Council

Receive progress reports on the corporate risk register at each meeting.

4. CORPORATE DIRECTORS AND HEADS OF PAID SERVICE

Overall responsibility for securing adherence to the Council's Policy on Risk Management, including Nick Baker having designation as the Council's Senior Risk Information Officer (SIRO) The description and responsibilities of this role can be found on the intranet.

5. CORPORATE LEADERSHIP TEAM (CLT)

Appoint a Corporate Director and Member to jointly take responsibility for risk management.

Agree the Corporate Risk Management Framework including the Policy Statement and Strategy.

Consider risks attached to proposals for new / changed policies and service delivery arrangements.

Ensure that this framework is applied.

## 6. RISK MANAGEMENT BOARD

See Terms of Reference (page 13) but amongst those is to:
Consider and agree the Council's corporate strategic risks and identify those requiring further action.

Allocate responsibility to Corporate Directors to develop action plans for corporate strategic risks.

Receive progress reports on risk reduction programme and propose revisions to "corporate risk register".

The Corporate Risk Register will be a standing item on the agenda (for any issues or changes that arise) and a full review of the register will take place every six months.

## 7. CORPORATE HEALTH AND SAFETY GROUP

Reports directly to the Risk Management Board and is charged with delivering health and safety policy across the Council.

## 8. CORPORATE RISK OFFICER

Coordinate risk management activity across the Council

Report on risk management activity to Risk Management Board, Corporate Leadership Team (CLT), Management Team and Members.

Maintain a corporate risk register and liaise with Service Managers relating to service risks. Ensuring that the service risks are update on the risk system every six months.

Provide risk management training for officers and Members, appropriate to their needs and responsibilities.

## 9. INDIVIDUAL SERVICE MANAGERS

Develop action plans in relation to corporate strategic risks as they relate to their area.

Identify risks attached to proposals for new / changed policies and service delivery arrangements.

Ensure that a service risk register is maintained and updated every six months on the risk system and that action plans are implemented.

## 10. EMPLOYEES

Maintain awareness of risk management principles and take responsibility for managing risk within their own working environment.

Apply risk management to those risks requiring further action, particularly new developments and "project" work.

Maintain a record of risk assessments undertaken relating to them and any resulting action plans.

## 11. INTERNAL AUDIT

Reporting to Management on the organisations performance under the Risk Management Framework.

## 12. EXTERNAL AUDIT

Reporting to Management via Use of Resources etc on the organisations performance on risk management.

# Document Information and Version Control

| | |
|---|---|
| Document Name | Risk Management Policy and Framework |
| Document Description | The framework outlines responsibilities for managing risks and defines how risk management should be applied across the Council. |
| Document Status | Under Review |
| Lead Officer | Duncan Ellis |
| Sponsor | Nick Baker |
| Produced by (service name) | Finance |
| Relevant to the services listed or all NNDC | All |
| Approved by | |
| Approval date | |
| Type of document | Policy and Framework |
| Equality Impact Assessment details | Not required |
| Review interval | Every 2 years |
| Next review date | |

| Version | Originator | Description including reason for changes | Date |
|---|---|---|---|
| 1 | Peter Gollop | | August 2010 |
| 1.01 | Helen Thomas | Transferred to policy template | 23 October 2015 |
| 1.02 | Helen Thomas | Marked up version showing out-of-date elements and suggested changes | 09/11/2015 |
| 1.03 | Karen Sly | Draft refresh presented to Audit Committee pending further review | February 2016 |
| 1.04 | Duncan Ellis | Updated provided to the Governance, Risk and Audit Committee | March 2017 |
| 1.05 | Duncan Ellis | Updated provided to the Governance, Risk and Audit Committee | March 2018 |