| | |
|---|---|
| **Information Risk Management Policy** | **19 September 2018** |
| **Audit Committee** | **For Approval** |

| **Linkage to Council Strategy (2015-19)** | |
|---|---|
| **Strategic Theme** | Leader and Champion/Protecting and Enhancing our Assets |
| **Outcome** | |
| **Lead Officer** | Director of Corporate Services |
| **Cost:** (If applicable) | |

## 1.0 Introduction

Purpose of report – to update the Risk Management Strategy, following General Data Protection Regulations (GDPR)

## 2.0 Background

2.1 In fulfilling its obligations as a Local Authority, Causeway Coast and Glens Borough Council will be exposed to various risks. The role of management within the organisation is to identify, manage and respond to these risks to reduce the likelihood of their occurrence and impact.

2.2 The Information Risk Management Policy forms part of the Causeway Coast and Glens Borough Council internal control and risk management strategy within a corporate governance framework. It has been developed to provide clarity and direction on current and future information risk management activity across the Council to ensure a consistent approach is taken to such risks.

2.3 Information that is collected, analysed, stored, communicated and reported on may be subject to theft, misuse, loss and corruption. The implementation of controls to protect information must be based on an assessment of the risk posed to the Council and must balance the likelihood of negative impacts against the resources required to implement the controls (and any unintended negative implications of the controls.

2.4 The Policy sets out the principles that the Council will use to identify, assess and management information risk in order to support the achievement of its planned objectives. It aligns with the corporate Council risk management strategy, framework and approach.

## 2.0 Detail

2.1 The Information Risk Management Policy and its supporting controls, processes and procedures applies to all information used, stored or disseminated within the Council, in all formats. This includes information processed by other organisations in their dealings with the Council.

2.2 This Information Risk Management Policy and its supporting controls, processes and procedures applies to all individuals who have access to Council information and technologies, including external parties that provide data processing services to the Council.

2.3 The Information Risk Management process will utilise the Council's overarching risk management approach and will operate in conjunction with the Council's overarching Risk Management Strategy

2.4 This Information Risk Management Policy provides a framework that will allow Causeway Coast and Glens Borough Council to improve upon the way in which it manages, stores and protects its information assets. This will be achieved through a proactive, ongoing process of information risk assessment, with the objective of improved prevention, control and containment of risk

## Recommendation

**It is recommended** that the Causeway Coast and Glens Borough Council Audit Committee approve the Information Risk Management Policy as detailed in Appendix 1.

# Causeway Coast and Glens Borough Council

# Information Risk Management Policy

## September 2018

| DOCUMENT CONTROL | | | |
|---|---|---|---|
| **Author** | **Moira Quinn** | | |
| **Version** | **1.0** | | |
| **Council Approval Date** | | | |
| **Review Date** | **As required** | | |
| **Approved By** | Chief Executive | **Signature** | |
| **Distribution** | **All Directors/Heads of Service for circulation to staff** | | |

# INFORMATION RISK MANAGEMENT POLICY

## TABLE OF CONTENTS

# 1.0 Purpose of the Policy

In fulfilling its obligations as a Local Authority, Causeway Coast and Glens Borough Council will be exposed to various risks. The role of management within the organisation is to identify, manage and respond to these risks to reduce the likelihood of their occurrence and impact.

Risk is inherent in all of the Council's activities. The delivery of the Council's objectives is surrounded by uncertainty, which poses threats to success and offers opportunity for increasing success. Risk is defined as the uncertainty of outcome, and good risk management should allow the Council to:

- Have increased confidence in achieving its desired outcomes;
- Effectively constrain threats to acceptable levels; and
- Take informed decisions about exploiting opportunities.

This Information Risk Management Policy forms part of the Causeway Coast and Glens Borough Council internal control and risk management strategy within a corporate governance framework. It has been developed to provide clarity and direction on current and future information risk management activity across the Council to ensure a consistent approach is taken to such risks.

Information that is collected, analysed, stored, communicated and reported on may be subject to theft, misuse, loss and corruption. The implementation of controls to protect information must be based on an assessment of the risk posed to the Council and must balance the likelihood of negative impacts against the resources required to implement the controls (and any unintended negative implications of the controls.

This Policy sets out the principles that the Council will use to identify, assess and management information risk in order to support the achievement of its planned objectives. It aligns with the corporate Council risk management strategy, framework and approach.

# 2.0 Policy Statement

Information Risk Assessment is a formal and repeatable method for identifying the risks facing an information asset. It is used to determine their impact and identify and apply controls that are appropriate and justified by the risks.

It is the Council's policy to ensure that information is protected from a loss of:

- **Confidentiality** – information will be accessible only to authorised individuals.
- **Integrity** – the accuracy and completeness of information will be maintained
- **Availability** – the information will be accessible to authorised users and processes when required.

# 3.0 Objectives

The main objectives of the Council's Risk Management Policy are to:

a) Provide a framework that enables Causeway Coast and Glens Council to identify, manage and treat information risks according to an agreed risk tolerance;
b) Safeguard the Council's information assets;
c) Ensure that our physical, procedural and technical controls are agreed by the information asset owner;
d) Ensure our physical, procedural and technical controls balance user experience and security;
e) Create an environment where all staff assume responsibility for risk management;
f) Ensure our physical, procedural and technical controls are cost-effective and proportionate.

The guidance contained within this strategy will provide a system for evaluating the known or potential risks to information within the Council and then categorising them into high, medium or low priorities.

All information risks will be captured within a document known as the Risk Register. The Council template is attached in Appendix 1. Action plans to eliminate the risks, or at least reduce them to an acceptable level will be developed. Each information risk identified will be classified according to its potential impact on Causeway Coast and Glens Borough Council and the likelihood of its occurrence. The risk evaluation framework is set out in detail in the next section of this document.

# 4.0 Definitions

## 4.1 Governance

HM Treasury defines governance as "the system by which an organisation directs and controls its functions and relates to stakeholders".

Recognising the importance of good governance in public bodies the Department of Finance and Personnel set out its decision that Northern Ireland Departments, like those of their GB counterparts, should adopt the key provisions of the Combined Code (incorporating Turnbull) in 2001.

One of the main changes that has arisen from adoption of this Code is the requirement for Accountable Officers to move from an annual Statement on Internal Financial Control to a much wider Audit and Governance Statement, not only covering financial control systems and associated risks but also other organisational control systems and associated risks.

### 4.2 Risk

In the Turnbull Committee Report it was stated that *'a sound system of internal control depends on a thorough and regular evaluation of the nature and extent of the risks to which the organisation is exposed.'* Therefore, effective risk management systems within the Council are also a key component of good internal control systems.

Risk management is defined as all the processes involved in identifying, assessing and judging risk, assigning ownership, taking action to mitigate risk and monitoring and reviewing risk control progress

### 4.3 Corporate Risks

A corporate risk is any risk, which would:

- Cause the organisation to fail to function
- Cause the organisation to fail to meet its key objectives
- Cause the organisation to fail to fulfil its duties or responsibilities
- Cause a significant loss of public confidence in the organisation
- Subject staff or the public to unreasonable levels of personal danger or threat to life or property
- Those risks which are assessed as 'Extreme'.

### 4.4 Information Risks

All potential threats to or vulnerabilities in information assets held by the Council whether natural or human, accidental or malicious.

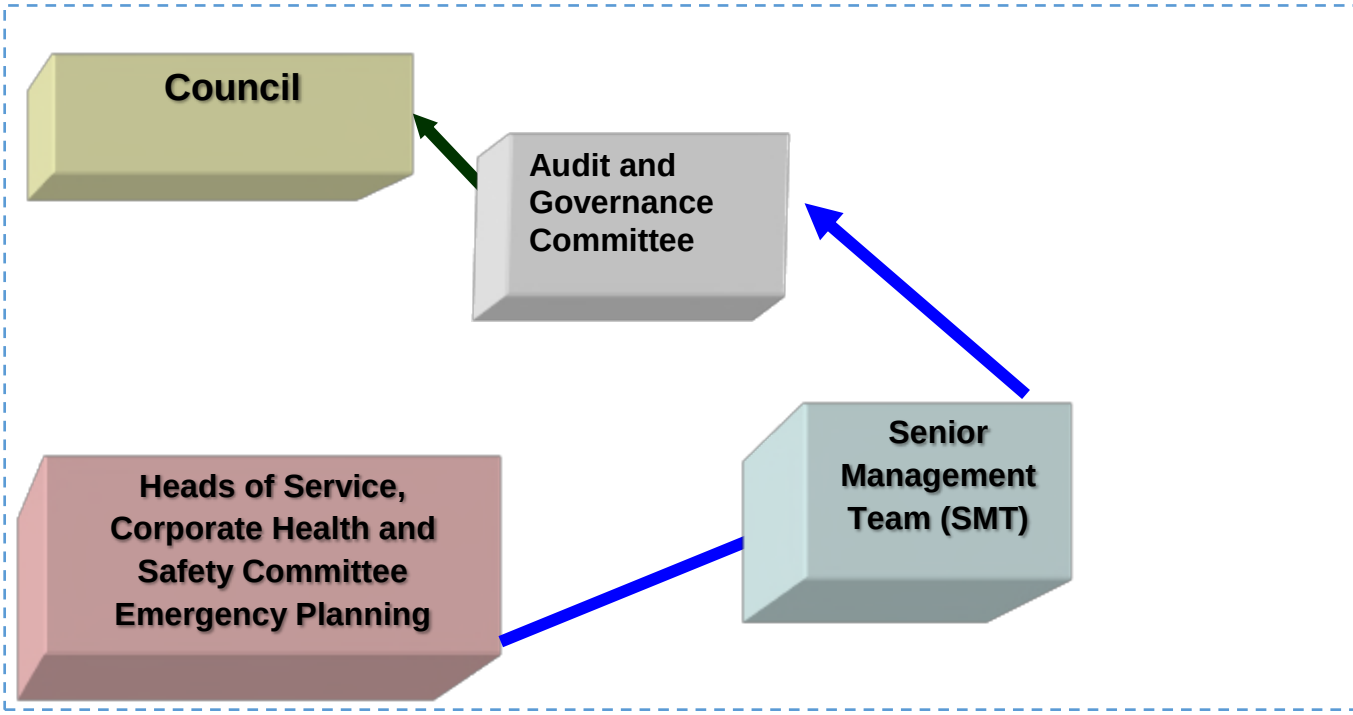
Examples of potential risks to Council's information assets are outlined in **Appendix 1**.

## 5.0 Scope of the Policy

This Information Risk Management Policy and its supporting controls, processes and procedures applies to all information used, stored or disseminated within the Council, in all formats. This includes information processed by other organisations in their dealings with the Council.

This Information Risk Management Policy and its supporting controls, processes and procedures applies to all individuals who have access to Council information and technologies, including external parties that provide data processing services to the Council.

# 6.0 Roles and Responsibilities




## 6.1 Audit Committee

The Audit Committee has overall responsibility for scrutinising the performance of the council in relation to Risk Management. The Audit Committee will meet quarterly.

## 6.2 Chief Executive

The Chief Executive has ultimate responsibility for ensuring that risks are properly managed and controlled in the Council. The Chief Executive is the Accountable Officer and is required to sign the Annual Governance Statement which encompasses financial and organisational risks. Day to day responsibility for implementation of the Strategy is however delegated down through the management structure to individual Directors, Heads of Service and Managers who are held accountable for ensuring that the requirements set out in this policy are implemented fully.

## 6.3 Director of Corporate Services

The Director of Corporate Services has operational responsibility for risk management particularly in relation to:

- Exercising oversight of the staff of Causeway Coast and Glens Borough Council responsible for the management of risk within the organisation.

- Providing assurance to Councillors that all identified risks are being managed.
- Providing SMT with regular briefings on all aspects of risk management
- Ensure the Risk Register is updated when new risks are identified and notified or when a change in circumstances concerning risks already in the register are notified to the Risk Management Co-Ordinator or Head of Service.
- Agree the ownership and management of risks
- Encourage proactive assessment and identification of new risks among staff members and keep them informed as to whether or not the risk will be included on the Risk Register.
- Encourage and assist in facilitating the training of staff to support the implementation of risk management procedures

### 6.4 Senior Management Team

SMT is responsible for ensuring good corporate risk governance across all Council services. Risk Management (including Information Risks) will be a standing item on the agenda at the monthly SMT meetings when corporate risk management issues will be discussed. The SMT is responsible for strategic planning with regards to risk management. Their purpose and remit in this field is to:

- Develop and review risk registers and action plans, at both Corporate and Service Level
- Decide on 'ownership' of risks.
- Raise awareness of risk throughout the Council, and within their own service area
- Provide education on risk throughout the Council, and within their own service area
- Effectively communicate risk issues within the Council, and within their own service area
- Monitor and review the risk management process and
- Respond to the changing nature of the risks faced by the organisation
- Managing the Risk Register (all corporate risks)
- Managing all EXTREME rated risks
- Reviewing Corporate risks
- Agreeing appropriate action
- Assigning responsibilities (individuals, departments etc)
- Monitoring the levels of Risk in the Council and by suitable analysis ensure that trends are detected, addressed and lessons learned
- Ensuring structures and processes are in place for Risk Management
- Monitoring the arrangements
- Ensuring that there are adequate resources available to risk manage effectively
- Reviewing the risk management arrangements annually
- Providing reports to the Council as required

- Receive reviews and reports from Directorate/Service Areas as and when required
- Review Annual Assurance Statements from Directorate/Service Areas
- Ensuring adequate communication processes are in place to keep all staff appropriately informed.

### 6.5 Directorate/Service Arrangements

Each Directorate/Service Area will review risks (including information risks) on a monthly basis or more frequently as required.

This review will include

- Management of the Service Risk Register/s
- Reviewing all service risks
- Agreeing appropriate action
- Assigning responsibilities
- Identifying trends and implementing suitable corrective actions and implement improvements through lessons learned
- Ensure Directorate/Service Risk Management arrangements are satisfactory
- Complete Annual Directorate/Service Assurance Statement

### 6.6 Employees

All employees have an individual responsibility to:

- Maintain an awareness of risk factors in their workplace.
- Participate in risk management education and training.
- Assist in risk assessments particularly within own work area
- Comply with Council policies and procedures.
- Notify the Director, through the Departmental/Service Working Group of identified risks and any changes to existing risks included on the risk register.
- Report all incidents to the Director/Head of Service.
- Manage risks, which they have been given responsibility for on the risk register.

### 6.7 Internal Audit

The Internal Audit function will audit the performance of Causeway Coast and Glens Borough Council to ensure that it has been successful in its management of risk in the context of this Guidance.

# 7.0 Delivery

The Chief Executive will have overall responsibility for the Information Risk Management Policy and any key activities associated with information risk management within Causeway Coast and Glens Council and subsequently seeking assurance from the SMT and the Director of Performance that all information risks are being effectively managed.

The information risk environment is constantly changing and developing as the Council's priorities and objectives develop. The information risk management process is therefore dynamic and on-going and will require constant review of risks to information assets and the consequent adjustment of controls to manage these risks. The principle adopted by this Policy is to ensure that the information risk management process is embedded into the structures of the Council at every level.

# 8.0 Information Risk Management Process

## 8.1 Risk Assessments

The Information Risk Management process will utilise the Council's overarching risk management approach and will operate in conjunction with the Council's overarching Risk Management Strategy.

The first step in the process will be the identification and analysis of any threats to and vulnerabilities of, Council's information assets. This will take the form of a "Risk Assessment".

Risk Assessments must be completed with an understanding of:

- The Council's business processes
- The impact on the Council of risks to information assets
- The technical systems in place to support information assets
- The legislation to which the Council is subject
- Up to date threats and vulnerability assessments.

A risk assessment exercise must be completed for:

- Every new information processing system (in conjunction with a Data Processing Impact Assessment for new systems capturing and processing personal data).

- Any modifications to systems or processes which could change the threats to or vulnerabilities of information assets.

- The introduction of a new information asset.

- Situations where there has been no review in the previous three years.

The information risk assessment process will follow the process outlined in **Appendix 2**. A risk score should ultimately be calculated using the Risk Ratings Matrix consistent with the system used by within the Council's overarching Risk Management Strategy.

### 8.2 Risk Registers

The Council's Service specific and Corporate Risk Registers will include the information risks identified from the risk assessment process.

All information risks will be assigned an owner (usually the Information Asset Owners) and a review date. Service specific risk registers will be held by Heads of Service and the Corporate Risk Register will be the responsibility of the Director of Corporate Services.

### 8.3 Risk Treatment

As outlined in the overarching Council Risk Management Strategy, information risks will include a risk treatment decision. The decision will fall into at least one of the following categories:

- Tolerate the Risk
- Treat the Risk
- Transfer the Risk
- Terminate the Risk

## 9.0 Training

The Council will provide suitable training in regard to information risk management, information risk identification, information risk assessment and information risk recording as required and provide assistance where specialised knowledge is necessary.

## 10.0 Evaluation and Review

Implementation of this Policy will be subject to audit by the Internal Audit function in the course of their normal cycle of audits.

The Information Risk Management Policy will be reviewed and updated annually by the Senior Management Team, and presented to Audit Committee for approval. Interim amendments may be required and communicated to all staff.

# 11.0 Conclusion

This Information Risk Management Policy provides a framework that will allow Causeway Coast and Glens Borough Council to improve upon the way in which it manages, stores and protects its information assets. This will be achieved through a proactive, ongoing process of information risk assessment, with the objective of improved prevention, control and containment of risk.

**Appendix 1**

# POTENTIAL RISKS TO COUNCIL'S INFORMATION ASSETS

| Risk Description | Causes | Effects | Active Controls |
|---|---|---|---|
| **Inappropriate disclosure of personal data** | Lack of identification of information assets containing personal data.<br><br>Lack of Awareness Training<br><br>Absence of appropriate Information Sharing Agreements<br><br>Failure to double check contents of materials proposed for disclosure.<br><br>Advice on disclosure not sought from DPO or Information Governance Officer. | Serious and unwarranted damage and distress to individuals.<br><br>Breach of GDPR/Data Protection Act<br><br>Regulatory action and potential financial penalties<br><br>Damage to reputation and integrity<br><br>Cost and Resources required to investigate. | Data Protection Policy<br>Information Risk Management Policy<br>Staff Training<br>Technological security<br><br>Audit of Information to map personal data<br>Staff Training |
| **Theft, loss or unauthorised access to information (ICT related)** | Inadequate access and permissions management.<br><br>Password sharing.<br><br>Poor information asset management | Serious and unwarranted damage and distress to individuals.<br><br>Breach of GDPR/Data Protection Act | Compliance with IT Security policies, Data Protection Policy, etc<br>Use of encrypted laptops and memory sticks.<br>Regular data backups carried out. |

| | | | |
|---|---|---|---|
| | Clear screen policy not enforced.<br><br>E-mails sent to wrong address<br><br>Inadequate business continuity planning | Regulatory action and potential financial penalties<br><br>Damage to reputation and integrity<br><br>Cost and Resources required to investigate.<br><br>Cost of recreating/retrieving information | Data Breach Response Plan in place |
| **Theft, loss or unauthorised access to information (hard copy systems)** | Inappropriate storage of documents resulting in their damage.<br><br>Documents not filed correctly and cannot be retrieved<br><br>Carelessness, dishonesty, sabotage.<br><br>Secure desk policy not enforced.<br><br>Documents posted/faxed to wrong address or lost/compromised during transmission. | Serious and unwarranted damage and distress to individuals.<br><br>Breach of GDPR/Data Protection Act<br><br>Regulatory action and potential financial penalties<br><br>Damage to reputation and integrity<br><br>Cost and Resources required to investigate.<br><br>Cost of recreating/retrieving information | Data Breach Response Plan in place.<br><br>Records Management Policy in place. |

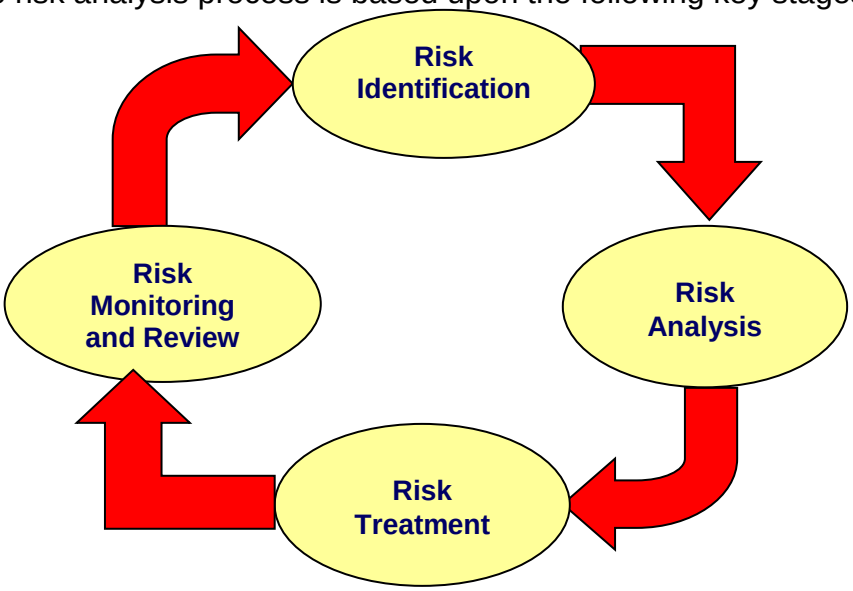
| | | | |
|---|---|---|---|
| **Information Assets lost as a result of fire, flood, server failure, etc.** | Business Continuity Plan not in place or information assets not considered in Business Continuity Plan. | Vital records destroyed.<br><br>Unable to access information with potential legal and financial consequences.<br><br>Significant investment required in rectifying situation.<br><br>Ability of Council to operate affected. | Audit of Information to identify records.<br><br>Business Continuity Plan in place with includes consideration of information assets.<br><br>Regular business continuity exercises carried out. |
| **Inadequate Records Management processes in place** | Records retained for wrong period of time or destroyed incorrectly.<br><br>Failure to create or locate records as evidence of business decisions and activities<br><br>Large volumes of data to be searched if information is requested.<br><br>Critical information cannot be found or found in a timely manner. | Unnecessary cost of storage of information.<br><br>Relevant records not available to protect Council's interests.<br><br>Premature destruction seen as an attempt to prevent disclosure.<br><br>Regulatory, court or financial penalties.<br><br>Damage to reputation and integrity. | Retention and Disposal Schedule in place.<br><br>Records Management Policy in place. |

**Appendix 2**

# Principles of Risk Analysis

A strategic approach to risk management depends on identifying risks against key organisational objectives. Risks relevant to these objectives are then considered and evaluated.

The risk analysis process is based upon the following key stages




## 5.1 Risk Analysis

Risk assessment/analysis uses descriptive scales to describe the magnitude of potential consequences/impacts and the likelihood that these consequences/impacts are realised. The risk levels are based on assessing the residual risk remaining bearing in mind any existing controls that have been identified and implemented. The overall risk is calculated by multiplying the probability and impact numbers to arrive at a Risk Rating.

## 5.2 Risk treatment

Risk treatment is concerned primarily with the following:

- Reducing the likelihood of the risk being realised
- Reducing or limiting the impact or consequences of the risk
- Transferring the risk e.g. insuring
- Accepting the risk
- Avoiding the risk

## 5.3 Risk Monitoring and Review

Risk Monitoring and review is concerned with examining the implementation of risk treatment plans and control measures. In effect auditing the effectiveness of the Councils risk action plans and making decisions if there is a need to do more. Evidence will include:

- Accident/incident reports, claims, staff turnover, theft losses etc
- Audits (both internally and externally), risk reviews.

The following are three important principles for analysing risk:

- Adopt a consistent approach throughout the organisation.
- Ensure that there is a clear process so that each element or level of risk identification fits into an overall structure.
- Establish a framework, approved by Senior Management, within which each risk is to be identified.

## 5.4 Risk Identification

Causeway Coast and Glens Borough Council identifies risks by applying a risk self-assessment model. In order to establish what the risks are it is useful to challenge circumstances through a number of simple questions such as

- What has happened in the past in similar circumstances?
- What have others experienced?
- What can go wrong?
- What are the dangers?
- What level of control is in place?
- What guidance is available?
- Apply approach of “In this situation, there is a risk that……” “So therefore we need to mitigate by……..”

## 5.5 Risk Evaluation

Each risk must be assessed to determine its potential impact and the likelihood of its occurrence. The combined assessment of impact and likelihood will enable the assignment of a ranking to a risk. The framework for the assessment of the impact, likelihood of occurrence and consequent risk ranking that will be adopted by the Council is set out in the risk impact matrix table below. The effect of the risk being realised will be expressed in terms of catastrophic (5), major (4), moderate (3) minor (2) and insignificant (1).

## 5.6 Risk Impact Matrix

The risk impact matrix is detailed in the table below. The table provides guidance on how to apply the impact criteria as detailed above.

| Category<br>**LEVEL OF IMPACT** | Personal Impact on Staff/Visitor/ Contractor | Technological/Quality / System Failure | Reputation and Public confidence Loss | Complaint Or Claim | Financial/ Assets/ Contractual Loss |
|---|---|---|---|---|---|
| **1. Insignificant** | No harm. | Negligible service deficit<br>Minor non-compliance<br>Easily recoverable/ repaired<br>No impact on service delivery<br>Minimal disruption to routine activity | No public/political concern. | Legal Challenge<br><br>Minor out-of-court settlement | Less than 1K |
| **2.** Minor | Minor harm or increased monitoring.<br>< 3-day absence for staff.<br>May involve more than one person. | Single failure to meet expected Council standards<br>Impact on organisation rapidly absorbed<br>No long term consequences | Local press interest.<br><br>Local public/political concern. | Civil action – Weak Defence<br><br>Improvement notice served<br><br>Difficult to justify action | £1K -£10K |
| **3. Moderate** | Treatment required, temporary significant harm,<br><br>RIDDOR reportable | More than one failure to meet expected Council standards or follow protocols<br>Impact on organisation absorbed with significant level of intervention<br>Minimal long term consequences | Limited damage to reputation<br>Extended local press interest/regional press interest.<br>Regional public/political concern. | Criminal prosecution or Civil action– Very weak defence<br><br>Prohibition Notice<br>No justification<br><br>Staff disciplined | £10K- £50K |
| **4. Major** | Near death or permanent harm.<br><br>Significant loss of staff morale | Failure to meet national/professional standards.<br>Impact on organisation absorbed with some formal intervention by other organisations<br>Significant long term consequences | Loss of credibility and confidence in organisation.<br>National press interest.<br>Independent external enquiry.<br>Significant public/political concern. | Criminal prosecution – no defence<br><br>Civil action – no defence<br><br>Staff dismissed | £50K – £500K |
| **5. Catastrophic** | Death | Gross failure to meet national standards<br>Impact on organisation absorbed with significant formal intervention by other organisations.<br>Major long-term consequences. | Full Public Enquiry.<br><br>Major public/political concern. | Criminal prosecution – no defence<br><br>Civil action – no defence<br><br>Staff fined or imprisoned | More than £500K |

## 5.7 Likelihood of Risk Occurring

The probability of the risk being realised is expressed in terms of Probable, Possible, Unlikely, Rare and Negligible using the definitions stated in the matrix below and in the context of existing controls being in place.

## 5.8 Likelihood of Risk Occurring Matrix

| Category | Probablility | Description |
|---|---|---|
| **1. Negligible** | 1 in 20,000 (Times) | Do not believe will ever happen |
| **2. Rare** | 1 in 2,000 (Times) | Do not expect to happen |
| **3. Unlikely** | 1 IN 200 (Times) | May Occur Occasionally |
| **4. Possible** | 1 in 20 (times) | Will Probably Occur |
| **5. Probable** | 1 in 10 (times) | Very Likely to Occur |

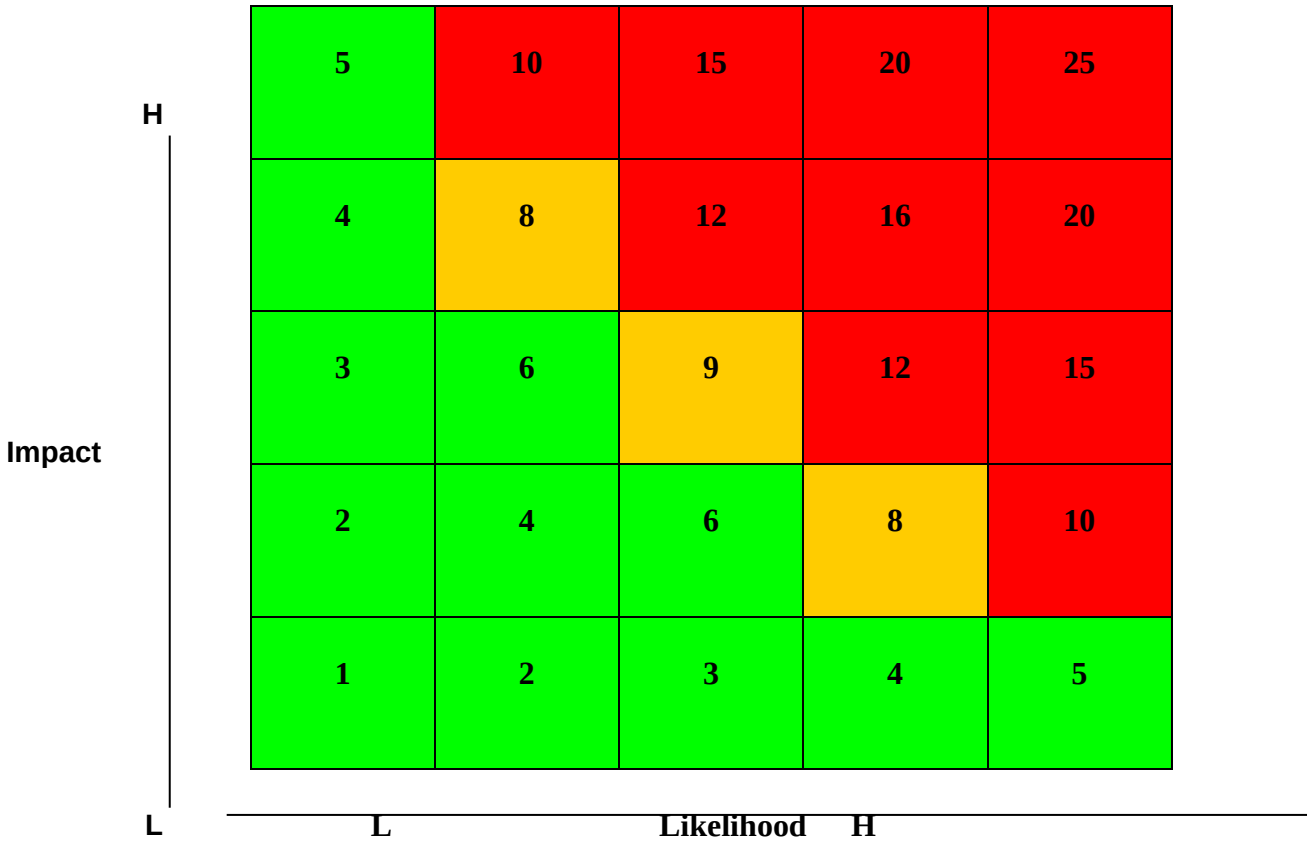
## 5.9 Risk Ranking

The risk ranking is expressed in terms of a numerical score from 1 to 25. The table below provides guidance in relation to the apportionment of the scores when assessing each risk.

**Risk ranking guidance scoring table**

| Rank | Indication | Action Required to manage the Risk |
|---|---|---|
| 1-6 | Low Risk | None – Keep risk under review |
| 7-9 | Moderate Risk | Additional action required to manage the risk effectively |
| 10-15 | High Risk | Urgent Action required to ensure effective management of the risk |
| 16-25 | Extreme Risk | Immediate Action required to ensure effective management of the risk. |

## 5.10 Risk Rankings Matrix




| Key | |
|---|---|
| **Rating** | **Descriptor** |
| **16-25** | **Extreme Risk (immediate action required** |
| **10-15** | **High Risk (Urgent Action required)** |
| **7-9** | **Moderate Risk (Action Required)** |
| **1-6** | **Low Risk (Keep Under Review)** |