

---

<b>Report To:</b>	<b>Audit Committee</b>	<b>Date:</b>	<b>24 October 2023</b>
<b>Report By:</b>	<b>Head of Legal, Democratic, Digital and Customer Services</b>	<b>Report No:</b>	<b>LS/103/23</b>
<b>Contact Officer:</b>	<b>Iain Strachan</b>	<b>Contact No:</b>	<b>01475 712210</b>
<b>Subject:</b>	<b>Revised Risk Management Strategy</b>		

---

## 1.0 PURPOSE

1.1  For Decision  For Information/Noting

1.2 The purpose of this report is to present an updated Risk Management Strategy to the Committee, for its consideration. Following the Committee's review of the Strategy it would go to the Policy & Resources Committee for approval.

## 2.0 RECOMMENDATIONS

- 2.1 It is recommended that the Audit Committee consider and provide feedback on the proposed revised Risk Management Strategy at Appendix 1.
- 2.2 It is recommended that the Audit Committee approve the Risk Management Strategy for onward submission to the Policy & Resources Committee.
- 2.3 It is recommended that the Audit Committee notes that the Corporate Risk Register will be reported to the Audit Committee in January 2024, followed by Policy & Resources Committee in February 2024.

**Iain Strachan**  
**Head of Legal, Democratic, Digital and Customer Services**

### **3.0 BACKGROUND AND CONTEXT**

- 3.1 There have been increasing pressures for public sector bodies to adopt formalised approaches to risk management.
- 3.2 In its Code of Practice, Audit Scotland makes it clear that the audited bodies are responsible for developing systems of internal control, including risk management, and for conducting annual reviews of the effectiveness of the system of internal control.
- 3.3 The Council developed a Risk Management Strategy in 2007 which provided a sound basis for risk management.
- 3.4 In 2010, the Corporate Risk Management Group, subsequently disbanded, reviewed the Risk Management Strategy and developed a Risk Assessment and Prioritisation Matrix to ensure consistency of practice and provide a useful tool to management in the achievement of goals and objectives.
- 3.5 The 2004 Best Value guidance was refreshed in 2020 and is structured around seven themes which include risk management as an integral part in demonstrating best value.
- 3.6 In January 2022 the Audit Committee approved a refreshed approach to risk management reporting arrangements which has provided an opportunity to review and update the risk management strategy. In addition, in June 2022 it was reported to the Committee that the Corporate Risk Register would be updated by July 2022. However, work capacity pressures have meant this work has not yet been completed.
- 3.7 Elsewhere on this agenda, the Audit Committee is considering the annual update on risk management activity for 2022/23.

### **4.0 PROPOSALS**

- 4.1 The Risk Management Strategy has now been reviewed and an updated revised version is attached at Appendix 1 for the Committee's consideration. Subject to the views of the Committee the Risk Management Strategy would then be submitted to the Policy & Resources Committee for approval.
- 4.2 Whilst there are no substantive changes to the Risk Management Strategy and operational procedures, there are some key aspects of the Strategy where revisions have been made which are worth highlighting to the Committee, these are:
  - The exclusion of Inverclyde Health and Social Care Partnership (IHSCP) from the Council's overall risk management monitoring and reporting arrangements, given the Inverclyde Integration Joint Board has its own strategic approach to risk management, and the operational activity flows from that.
  - A Corporate Risk Management Group has been established, chaired by the Chief Executive, the aim of this group being to steer the direction of the Council's overall approach to risk management and provide a clear mechanism for ongoing monitoring and review. The members of the Group will act as conduits between the CMT and Directorate/Service risk management operations. The senior officer nominated to chair the Corporate Risk Management Group.
  - A new Corporate Risk Adviser post has been created, agreed to by the CMT. This post will be jointly funded by the Council and the IHSCP, to provide the operational advice and support that is required to further embed risk management into operational activity and enable service areas to fulfil their risk management duties under the Risk Management Strategy, including in their use of Pentana for risk register recording. Given the joint funding, this post will also provide that operational support to IHSCP.

- 4.3 The Corporate Risk Register is in the course of being reviewed, and it is intended that it will be reported to the Audit Committee in January 2024, followed by Policy & Resources Committee in February 2024. Going forward, the Corporate Risk Register will be reported 6 monthly to CMT and annually to the Audit Committee and the Policy & Resources Committee.
- 4.4 It has been recognised by the CMT that work is needed, across all Council service areas, to ensure the Council's approach to risk management is suitably robust and embedded in operational activity. It is envisaged that the revisions to the Strategy, coupled with the operational changes summarised above, will provide that additional focus. This will, however, be monitored by CMT, and through the Corporate Risk Management Group.

## 5.0 IMPLICATIONS

- 5.1 The table below shows whether risks and implications apply if the recommendation is agreed:

SUBJECT	YES	NO
Financial	X	
Legal/Risk	X	
Human Resources	X	
Strategic (LOIP/Corporate Plan)	X	
Equalities, Fairer Scotland Duty and Children/Young People's Rights & Wellbeing		X
Environmental & Sustainability		X
Data Protection		X

## 5.2 Finance

### One off Costs

Cost Centre	Budget Heading	Budget Years	Proposed Spend this Report	Virement From	Other Comments
N/A					

### Annually Recurring Costs/ (Savings)

Cost Centre	Budget Heading	With Effect from	Annual Net Impact	Virement From (If Applicable)	Other Comments
Legal Services	Employee Costs	1.1.24	£60k		£30k funded from Insurance Charges and £30k from IHSCP

## Legal/Risk

### 5.3

Having an up-to-date risk management strategy demonstrates that the Council is taking ownership of risk management so that effective measures are put in place for managing risk. The current approach to risk management allows the Council to demonstrate a clear understanding of the risk profile of the organisation, but work is required across all service areas to ensure this approach is embedded and being actioned, with suitable internal reporting.

## 5.4 **Human Resources**

The human resources implications are set out in this report.

### **Strategic**

- 5.5 This report helps ensure strong governance, and its findings will help support delivery of the Council Plan adopted by Inverclyde Council on 20 April 2023, and in particular outcome theme 3: Performance, with the Council seeking to provide high quality and innovative services that deliver value for money.

## 6.0 **CONSULTATIONS**

- 6.1 Relevant officers have been consulted in the review and update of the risk management strategy, including the Corporate Management Team.

## 7.0 **LIST OF BACKGROUND PAPERS**

- 7.1 None



**Risk Management Strategy**

24 October 2023  
V4.3

## **CONTENTS**

### Section

<u>Section</u>		<u>Page</u>
1	Introduction and Purpose	2
2	Risk Management Policy Statement	2-4
3	Interfaces	4-5
4	Risk Context	5-7
5	Risk Identification	7
6	Assessment, Prioritisation and Management of Risk	7
7	Assigning Ownership	8
8	Risk Review	8
9	General	9
10	Communications	9
	Appendix 1 – The Risk Management Cycle	
	Appendix 2 - Roles and Responsibilities	
	Appendix 3 – Risk Assessment and Prioritisation Framework	

## **1. INTRODUCTION AND PURPOSE**

- 1.1 Risk management is defined in the Institute of Risk Management Risk Management Standard as follows:-

*“Risk Management is a key part of an organisation’s strategic management. It is the process whereby organisations methodically address the risks attached to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities.”*

- 1.2 Due to the recognised importance of managing risks as stated above, there is an expectation for public sector organisations to have adopted formalised approaches to risk management. These expectations emanate from, among other things, the Combined Code and the CIPFA/Solace publication on corporate governance best practice entitled “Delivering Good Governance in Local Government”.
- 1.3 In addition, Audit Scotland in its Code of Audit Practice makes it clear that the audited bodies are responsible for developing and implementing systems of internal control, or internal financial control, including risk management, and for conducting annual reviews of the effectiveness of the system of internal control.
- 1.4 Furthermore, the 2004 Best Value guidance was refreshed in 2020 and is structured around seven themes which include Risk Management as an integral part of demonstrating Best Value.
- 1.5 The purpose of this Strategy is to clearly define Inverclyde Council’s approach to Risk Management and support officers and Members in managing risks and opportunities effectively, putting them in a stronger position to deliver the corporate objectives.
- 1.6 The Risk Management Strategy will therefore be an essential element of the strategic planning processes and will be focused around corporate and Committee objectives. The Strategy will focus on detailing the processes for identifying, assessing, evaluating and managing the risks that face the organisation and how these will assist in the delivery of the corporate goals.

## **2. RISK MANAGEMENT POLICY STATEMENT**

### **2.1 Policy statement**

Inverclyde Council is dedicated to the management of risks within its control to enhance the Corporate Governance process, and in doing so aims to:-

- ◆ Identify, assess and manage risks;
- ◆ Safeguard the Council’s assets; and
- ◆ Enhance the delivery of its services to the Community.

## 2.2 Aim

The aim of this Strategy is to deliver a consistent, effective framework and approach for managing risks across the organisation at all levels. This will aid the achievement of Inverclyde Council's corporate goals.

The approach is to use best practice tools and techniques to manage the risks that the Council faces, with the aim of reducing the level of risk in the organisation to a tolerable level.

The Strategy aims to focus on the organisation's processes, and looks to raise the awareness of risk and its importance throughout the organisation, enabling front line staff, managers and directors to identify and manage risk in a controlled environment. It is also intended to make risk management an integral part of the strategic planning process through the Committee Delivery Plans.

## 2.3 Objectives

To facilitate the effective delivery of the Risk Management Strategy, the following objectives have been identified:-

- to deliver more effective financial and resource management, and maintain effective stewardship of public funds;
- to meet statutory responsibilities;
- to minimise the Council's exposure to risk and potential loss;
- to promote and support health and safety, welfare issues and appropriate people management both internally and externally;
- to promote a more risk aware culture for employees and Elected Members;
- to improve and enhance service delivery;
- to achieve better forward planning through identifying and prioritising risks;
- to protect and promote a favourable corporate image; and
- to embed robust systems for identifying and evaluating significant risks.

## 2.4 Outputs

The Council aims to demonstrate the achievement of these objectives by:-

- Including Risk Management as an integral part of its management processes and day-to-day operations through corporate, committee and service delivery plans;
- Ensuring sound systems of internal control;
- Incorporating Risk Management into major service reviews including Best Value and project management;
- Preparing contingency plans in areas where there is a potential for serious adverse effects on service continuity;
- Regular monitoring and review of arrangements; and
- Ensuring that legislative responsibilities in relation to the management of risk are responded to and met.



## 2.5 Scope

The Risk Management Strategy is directly applicable to the Council's Directorates and Services as follows:-

<b>Directorate</b>	<b>Services</b>
Chief Executive	Finance Services; Legal, Democratic, Digital and Customer Services
Education, Communities and Organisational Development	Education; Culture, Communities and Education Resources; OD, Policy and Corporate Communications
Environment and Regeneration	Physical Assets; Regeneration, Planning and Public Protection

Where appropriate, strategic partnerships and specific projects will also be covered by the strategy, following due engagement with partners to develop and deliver the risk management requirements in these areas. As noted below, the Inverclyde Health & Social Care Partnership has its own risk management arrangements.

## 3. INTERFACES

3.1 Risk Management is part of the overall Corporate Governance framework for the Council. While the responsibility for risk management policy development and co-ordination lies in Legal, Democratic, Digital and Customer Services and is co-ordinated by the Head of Legal Democratic, Digital and Customer Services, there are a number of key interfaces that must be managed to support the effective transition of risk management across the Council.

### 3.2 Internal Audit

The Internal Audit service provides an independent and objective assurance and advisory service to management and the Audit Committee. The assurance role of Internal Audit is to provide an opinion the adequacy and effectiveness of the processes by which risks are identified, prioritised, managed, controlled, mitigated and reported.

### 3.3 Insurance

While the overall Risk Management Strategy is not insurance driven, insurance is one form of response the Council adopts to manage risk. By implementing effective risk management, Inverclyde Council should be better placed in the insurance market to achieve cost effective premiums. Therefore, close liaison will be required with the insurance team in Finance to review the number and types of claims, and trends as risk management becomes embedded.

### **3.4 Health & Safety**

Inverclyde Council has made a significant investment in terms of having qualified staff with a Corporate Health and Safety team.

The Health & Safety function sits within the OD, Policy and Communications service but there is clearly a need for Health & Safety and risk management to interface. While specific Health & Safety risk assessments must continue to be conducted, major risks should be included in the service risk registers. Therefore, the Corporate Risk Adviser and the Health and Safety team leader will meet regularly to review common areas of risk to support the achievement of best practice, and escalate any identified areas of concern to the Head of Legal Democratic, Digital and Customer Services and the Head of OD, Policy & Communications.

### **3.5 Civil Contingencies**

The Civil Contingencies Act 2004 came into effect in Scotland in various stages between 2004 and 2006. The specific Regulations made under the Act are the Civil Contingencies Act 2004 (Contingency Planning) (Scotland) Regulations 2005, which came into effect in November 2005. This legislation requires local authorities to have business continuity strategies and plans in place and tested. Risk management ties in with business continuity management in the low probability, high impact risks which, if they occur, could constitute an emergency situation for the Council, potentially resulting in key services or systems failing. The Council operates a shared civil contingencies planning arrangement with Renfrewshire, East Renfrewshire and West Dunbartonshire Councils.

### **3.6 Physical Assets**

The Assets Team, within Physical Assets, is responsible for the operational management and control of the Council's property portfolio and requires to demonstrate compliance with various regulatory requirements encompassing, for example, electrical installation, PAT testing, asbestos management, Disability Discrimination Act compliance, gas installations and fire assessments. Due of the inherent risks in these operations, and the need for appropriate and consistent corporate responses it is important that the Assets Team engage in the Council's risk management process through participation in the Corporate Risk Management Group. This will allow structured discussion on property issues in the context of risk management as a whole.

### **3.7 Inverclyde Integration Joint Board**

Whilst the Council and the Inverclyde Health & Social Care Partnership share a corporate risk adviser post, the Inverclyde Integration Joint Board's Integration Scheme sets out its own responsibilities for risk management, and it is this to which services within the Inverclyde Health & Social Care Partnership will have reference to, and not this Risk Management Strategy.

## RISK CONTEXT

- 4.1 The Risk Management Strategy is objective driven, and the risk registers will clearly link to the corporate, committee and service objectives and plans.

The complete integration of risk management into the culture of the organisation can only be achieved through the full commitment and understanding of all stakeholders, including:-

- ◆ Elected Members;
- ◆ Corporate Management Team;
- ◆ Senior Managers; and
- ◆ All Council Officers.

All of these stakeholders have a role to play in the control environment within which the Council operates, whether in connection with policy setting and decision making, the accountability challenge process, the implementation of Council objectives, setting of internal controls or the provision of a safe working environment.

Ultimate responsibility for the delivery of Council objectives lies with the Council, Chief Executive and the Council's Corporate Management Team (CMT).

To take the agenda forward, the Chief Executive has lead responsibility for Corporate Risk Management.

Operationally, a Corporate Risk Management Group (CRMG) will be established to steer the development of the overall approach and to provide a mechanism for ongoing monitoring and review. CRMG members are required to be of appropriate seniority and experience, and are identified and nominated by Directors to represent the interests of the Directorate or of specific Services within each directorate.

The Chief Executive, or an alternative senior officer responsible to the Chief Executive, chairs the quarterly meetings of the CRMG.

The role of the CRMG members has been defined as being to act as representatives of their directorates and provide a conduit between the Corporate Management Team and directorate/service risk management operations.

The terms of reference for this group are as follows:-

- To develop and embed risk management as part of the culture of the Council.
- To monitor the risk profile of the organisation against the Council's desired risk appetite.
- To monitor the effectiveness and output of the risk management process.
- To assess the overall population of risk within the Committee Delivery & Improvement Plan and service risk registers, including any changes during the period.
- To consider and challenge risk prioritisation as provided by the risk owners, including discussion of any perceived discrepancies.
- To prioritise and accelerate those risk management strategies that are critical to the achievement of corporate objectives.
- To ensure that risk management is appropriately embedded within line management and that this process is monitored.
- To reach agreement on the significant matters arising in the period that should be brought to the attention of the CMT and Audit Committee.
- To monitor the effectiveness of Council wide policies and to feed into strategy development and review.
- To review the results of internal audit reviews and reviews by external bodies.

- To provide a mechanism for risk management issues to be discussed and disseminated to all areas of the Council, with a view to sharing good practice.

Reports from the CRMG are submitted to the Corporate Management Team on at least an annual basis.

Regular risk management updates are provided to the Audit Committee, with a Risk Management Annual Report being presented to Members after the end of each financial year.

## 5. RISK IDENTIFICATION

This stage can be separated into two distinct phases:

**Initial risk identification** – for Directorates or services that have not previously identified risk in a structured way.

**Continuous risk identification** – to identify new risks that did not previously arise, changes to existing risks and risks which have ceased to be relevant.

In either case, risks should be related to the Council's corporate objectives and be considered at both a strategic and operational level. Strategic risks focus on identifying the key barriers to successful achievement of the Council's objectives. Operational risks are more likely to focus on continuity of business services.

**Common Areas of Risk are:**

<b>Strategic</b>	Doing the wrong things as an organisation. Missing opportunities.
<b>Financial</b>	Losing resources or incurring liabilities.
<b>Reputational</b>	The Council's image. Loss of public confidence.
<b>Political</b>	Political embarrassment. Not delivering on local or national policies.
<b>Partnerships</b>	Specific risks to the Council as a result of being in a partnership.
<b>Legal/Regulatory</b>	Claims against the Council. Non-compliance.
<b>Operational</b>	Service delivery failure, targets missed.
<b>Information</b>	Loss of, or inaccurate data, systems or reported information.
<b>Customer/citizens</b>	Understanding their needs, delivery of services.
<b>Environmental</b>	Things outside of our control. Environmental impact of the Council.
<b>People</b>	Employees, management, Members, Chief Officers.

Not all services of the Council will have risks under all these categories.

## 6. ASSESSMENT, PRIORITISATION AND MANAGEMENT OF RISK

The Council has adopted a clear structured process for risk assessment for which both impact and likelihood are considered.

Some types of risks allow objective analysis eg financial risks whereas others may be more subjective eg risk to reputation. This assessment matrix allows for assessing all types of risk and considers the perspectives of the whole range of stakeholders likely to be affected.

The assessment is carried out by evaluating the impact if the risk is realised and the likelihood of the risk being realised.

A framework document which outlines the Council's approach is attached at Appendix 3.

## **7. ASSIGNING OWNERSHIP**

Once the risks have been assessed and the most appropriate treatment strategy chosen, an individual risk owner needs to be nominated.

Risk ownership is fundamental to the risk process as it identifies the person best placed to manage and influence the risk.

The owner will be accountable for either managing out the risk or reducing it to an acceptable level. Risk ownership needs to be assigned to individuals. Where the risk impacts across different areas, ownership will still be assigned individually, with nominated individuals assisting in the management of the risk.

Risk owners may delegate some actions to reduce or contain the risk, but they are still ultimately accountable to ensure the risk is controlled.

## **8. RISK REVIEW**

8.1 Risk has to be reviewed and reported on for the following important reasons:

- To monitor whether or not the risk profile is changing;
- To gain assurance that risk management is effective; and
- To identify to both the Council and Corporate Management Team where and when further action is required.

With this in mind a risk reporting framework has been developed.

### **8.2 Risk Registers**

Risk registers have been developed at corporate, committee, directorate, service and (where appropriate) project level. The risk registers, as a minimum, will contain:-

- A list of risks including their associated factors and consequences;
- The assessment of the likelihood and impact of the risks;
- The agreed strategy for treating the risk and the actions and control measures to be adopted;
- The acceptable level of risk after the controls have been implemented; and
- Details of the nominated risk owner.

The use of formal risk registers and risk progress reports will provide an effective basis for risk reporting and will provide a compliant audit trail.

### **8.3 Corporate Risk Reporting**

To enable a complete assessment of the overall risks across the Council the reporting process is as follows:

A three staged process for the reporting of risk.

1. Following the completion of the risk management process in the service area the appropriate Head of Service and Director will sign off completed risk registers, as a true and accurate reflection of the risk exposure within the service area.
2. The registers will be presented at CRMG to establish if the associated level of risk is acceptable for the service. If the tolerance level of the risk is deemed to be too high, the CRMG will advise what tolerance level should be adopted and what appropriate action is to be taken by the service to reach the required level.
3. Each Committee register will also be presented to the Corporate Management Team and appropriate service committee for discussion and comment as part of the CDIP reporting process.

The Head of Legal Democratic, Digital and Customer Services will be responsible for compiling a Corporate Risk Register for the Council as a whole, taking the risk registers signed off by Heads of Service and Directors. This corporate risk register will be reported to the CMT on a 6 monthly basis, and following a full review reported to the Audit Committee and Policy & Resources Committee on an annual basis at the start of each calendar year.

The reporting process will allow the Council to determine both the individual and corporate risk tolerance levels across the organisation, meet corporate governance requirements and demonstrate to the Council the service areas of greatest risk exposure.

## **9. GENERAL**

9.1 As risk management is being rolled out and embedded throughout the Council, it is imperative that staff, managers, heads of service, directors and Elected Members understand its principles and how these are adopted in practice.

### **9.2 Raising risk awareness**

It is intended to provide risk management training as part of the corporate induction process for employees. Risk Management training is provided to Members on a regular basis as part of ongoing CPD requirements.

### **9.3 Tailored/Specific Training**

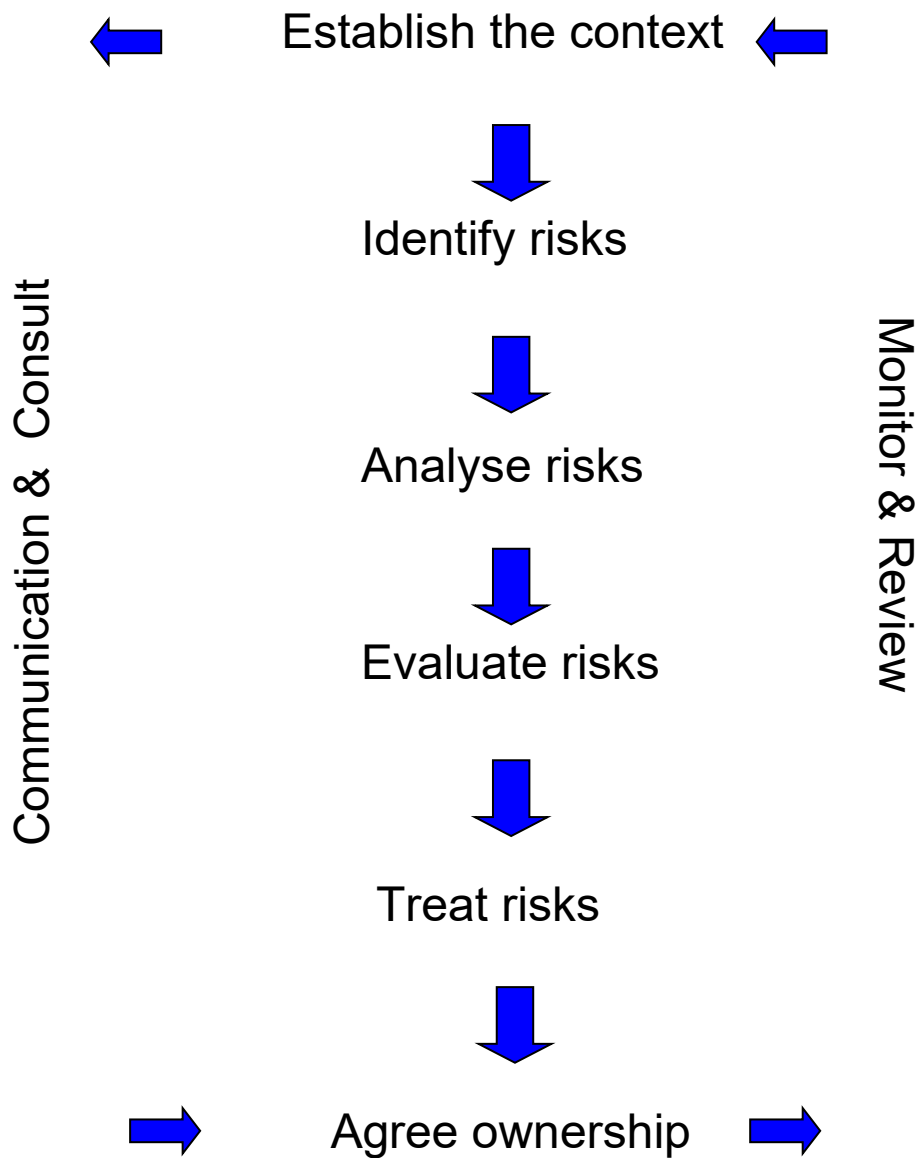
If a service identifies there are specific training requirements, a tailored training package will be designed and delivered to meet the required needs.

## **10. COMMUNICATIONS**

So that the corporate Risk Management Strategy is communicated to as wide an audience as possible, a communications process has been developed. Once approved, a copy of the Strategy will be made available on the intranet and cascaded to service areas.

A series of briefings will also be undertaken to communicate the Strategy through the Service Management Teams.

# Risk Management Cycle



## Roles & Responsibilities

### The Council (through the Audit Committee and the Policy & Resources Committee)

- The role of the Council is to approve or ratify the Risk Management Strategy which will reflect the Council's risk appetite.
- The Council has responsibility to scrutinise policy effectiveness and review performance.

### Chief Executive

- Provide strategic leadership that endorses the Council's Risk Management Strategy and plan, driving forward the identification and review of top risks.
- Responsibility for sign off and agreement of the Corporate Risk Register.

### Directors

- Each director is responsible for ensuring that risks have been properly identified and assessed across all their work areas, particularly cross cutting risks.
- Responsible for agreeing risk register returns for their directorates, ensuring that Heads of Service actively address risks in their command and escalate risk upwards as appropriate.
- Personal ownership of relevant Corporate risks and effectively address and report on their progress.

### Corporate Management Team

- Determine and ratify risk policy and strategy.
- Set strategic direction.
- Define risk appetite.
- Ensure arrangements are in place to maintain a sound system of internal control.
- Consider the effectiveness of the system of internal control.
- Corporate responsibility for ownership of Risk Management Strategy and implementing the approach to managing risk and strategically reviewing the Council's key risks.
- Key risks to be agreed, owned and addressed by CMT.



## **CRMG**

- Implementing policies on risk management and internal control;
- Identifying and evaluating the significant risks faced by the Council for consideration by the Audit Committee of the Council;
- Monitoring the management of significant risks to ensure these are appropriately mitigated;
- Satisfying itself that the less significant risks are being actively managed, with the appropriate controls in place and working effectively;
- Providing adequate information in a timely manner to the Chief Executive and appropriate Committee on the status of risks and controls;
- Undertaking an annual review of effectiveness of the system of internal control and reporting on this to the Chief Internal Auditor, as part of their annual assurance review that is reported to the Council through the Audit Committee;
- setting policy and strategy for risk management;
- primary champion of risk management at strategic and operational level;
- building a risk aware culture within the organisation, including appropriate education;
- establishing internal risk policy and structures for directorates and services;
- designing and reviewing processes for risk management;
- co-coordinating the various functional activities which advise on risk management issues within the organisation;
- developing risk response processes, including contingency and business continuity programmes; and
- preparing reports on risk for the Audit Committee and the stakeholders.

## **Directorate Management Teams**

- Nominating risk owners for the identified key risks.
- Regular review of risk profile and policy effectiveness.
- Accountable to the Chief Executive for monitoring the system of internal control and providing assurance to the Chief Executive/CMT that it has done so.
- Assessment of the effectiveness of the management of individual risks through quarterly monitoring of the directorate risk register.

## **Heads of Service**

- Responsible for the review of key service risks.
- Responsible for embedding risk management across their services and identifying the priority risks in their command and particularly cross-cutting risks.

## **Head of Legal Democratic, Digital and Customer Services (Risk Management Responsibilities)**

- Provide advice and guidance on risk management for both Officers and Elected Members of the Council in meeting their risk management responsibilities.
- Develop and co-ordinate the delivery of this Risk Management Strategy and annual plan across the Council and review its effectiveness.

## **Line Managers**

- General responsibilities to ensure staff are familiar with the latest risk management policy, strategy and guidance.
- Ensure that where staff have risk management responsibilities, this is reflected in their work objectives.
- Responsibility to act upon risks identified by staff which cannot be managed at employee level.

## **Audit Committee**

- Responsible for reviewing and agreeing the processes for managing risk in the Council.
- Allocating risk as an agenda item as often as required and no less than twice a year at committee and receiving feedback from the Head of Legal Democratic, Digital and Customer Services on implementation and performance of the risk process.
- Responsible for advising the Council on the performance of the processes and how effectively risk management is being embedded across the organisation.

## **Chief Internal Auditor (Audit Responsibilities)**

- Responsible for auditing the risk management process across the organisation and assessing the effectiveness of its application.
- Identifying through the audit process areas of strength, weakness and non-compliance, advising on improvement areas.

## **Heads of Service (Risk Co-ordinator responsibilities)**

- Co-ordinate with services and- Head of Legal Democratic, Digital and Customer Services over the details within risk registers.
- Update Pentana on significant changes to risk description, score, additional mitigations and new risks identified.
- Provide general feedback to CMT and Head of Legal Democratic, Digital and Customer Services on the implementation of the Risk Management Strategy and the various risk processes at local level.
- Focal point for cascading revisions to the central guidance of useful risk related information.

## **All Staff**

- All staff are responsible for maintaining an awareness of risks inherent in their jobs and reporting to their line manager any risks that they are unable to manage.

## **Risk Owners**

- Risk owners are accountable for managing the risks assigned to them in the risk register. While risk owners may delegate responsibility to others for action to control the risk, they are ultimately responsible for the risk.



**RISK ASSESSMENT AND PRIORITISATION FRAMEWORK**

**OCTOBER 2023**

**VERSION 1.0**

## Risk Assessment and Prioritisation Framework

---

<b>CONTENT</b>	<b>PAGE</b>
1 Introduction	2
2 Identification of Risk	3
3 Assessment and Prioritisation of Risk	3
4 Management and Control of Risk	8
5 Review and Reporting	10

## Risk Assessment and Prioritisation Framework

---

### 1 Introduction

Risk management is an integral part of corporate governance and sound management. The effective identification, assessment and management of risk is key to helping organisations be successful in delivering their objectives whilst protecting the interests of their stakeholders.

Effective risk management will allow the Council to:

- Have increased confidence in achieving its desired outcomes.
- Contain threats to an acceptable level.
- Take informed decisions about exploiting opportunities.

This document describes the Framework within which risks will be assessed and monitored by Inverclyde Council and provides a step-by-step guide. It should be read in conjunction with the Council's Risk Management Strategy.

The Framework will allow Directorates and Services to:

- Undertake risk assessment properly and frequently as a natural way to communicate and plan for improvement.
- Better appreciate their role in managing the strategic and operational risks in their particular area of responsibility.
- Have a good understanding of their role in demonstrating risk is managed to acceptable levels.

There are four main stages to the risk assessment process:

- **Identification** – the means by which threats and opportunities are identified.
- **Assessment** – estimating the levels of impact and likelihood of the risks and opportunities and assessing which risks pose the greatest threat.
- **Management and Control** – developing and putting into place actions and control measures to manage the risk.
- **Review and reporting** – monitoring that the actions and control measures are appropriate, effective and still relevant, identifying changes in circumstances and environment and checking the effect on risk priorities, reporting on progress to the Council.

This document deals in turn with these four stages, describing processes, responsibilities and timescales.

## 2 Identification of Risk

This stage can be separated into two distinct phases:

**Initial risk identification** – for Directorates or services that have not previously identified risk in a structured way.

**Continuous risk identification** – to identify new risks that did not previously arise, changes to existing risks and risks which have ceased to be relevant.

In either case, risks should be related to the Council's corporate objectives and be considered at both a strategic and operational level. Strategic risks focus on identifying the key barriers to successful achievement of the Council's objectives. Operational risks are more likely to focus on continuity of business services.

### Common Areas of Risk are:

<b>Strategic</b>	Doing the wrong things as an organisation. Missing opportunities.
<b>Financial</b>	Losing resources or incurring liabilities.
<b>Reputational</b>	The Council's image. Loss of public confidence.
<b>Political</b>	Political embarrassment. Not delivering on local or national policies.
<b>Partnerships</b>	Specific risks to the Council as a result of being in a partnership.
<b>Legal/Regulatory</b>	Claims against the Council. Non-compliance.
<b>Operational</b>	Service delivery failure, targets missed.
<b>Information</b>	Loss of, or inaccurate data, systems or reported information.
<b>Customer/citizens</b>	Understanding their needs, delivery of services.
<b>Environmental</b>	Things outside of our control. Environmental impact of the Council.
<b>People</b>	Employees, management, Members, Chief Officers.

Not all services of the Council will have risks under all these categories.

## 2 Identification of Risk (Continued)

When considering risk, typical phrasing could be:

Loss of ...	leads to ...	resulting in ...
Failure of ...		
Lack of ...		
Partnership with ...		
Development of ...		

## 3 Assessment and Prioritisation of Risk

The Council has adopted a clear structured process for risk assessment for which both impact and likelihood are considered.

Some types of risks allow objective analysis eg financial risks whereas others may be more subjective eg risk to reputation. This assessment matrix allows for assessing all types of risk and considers the perspectives of the whole range of stakeholders likely to be affected.

The assessment is carried out by evaluating the impact if the risk is realised and the likelihood of the risk being realised.

For Inverclyde Council, we have adopted a 5 x 5 scale for impact and likelihood as follows:



### 3 Assessment and Prioritisation of Risk (Continued)

#### Risk Impact

	<b>1 Insignificant</b>	<b>2 Minor</b>	<b>3 Moderate</b>	<b>4 Major</b>	<b>5 Catastrophic</b>
<b>Financial</b>	<£100k	£100k-£250k	£250k-£500k	£500k-£1,000k	£1,000K>
<b>Reputation</b>	Individual negative perception	Local negative perception	Intra industry or regional negative perception	National negative perception	Sustained national negative perception
<b>Legal and Regulatory</b>	Minor regulatory or contractual breach resulting in no compensation or loss	Breach of legislation or code resulting in a compensation award	Regulatory censure or action, significant contractual breach	Breach of regulation or legislation with severe costs/fine	Public fines and censure, regulatory veto on projects/withdrawal of funding. Major adverse corporate litigation.
<b>Operational/Continuity</b>	An individual service or process failure	Minor problems in specific areas of service delivery	Impact on specific customer group or process	Widespread problems in business operation	Major service or process failure impacting majority or major customer groups

#### Likelihood

	<b>1 Rare</b>	<b>2 Unlikely</b>	<b>3 Possible</b>	<b>4 Probable</b>	<b>5 Almost Certain</b>
<b>Definition</b>	Not likely to happen in the next 3 years	Unlikely to happen in the next 3 years	Possible to occur in the next 3 years	Likely to occur in the next year	Very likely to occur in the next 6 months

### 3 Assessment and Prioritisation of Risk (Continued)

The first assessment of risk levels against these criteria should take no account of any measures or factors that may be in place to control the risk. This establishes the level of “inherent risk”.

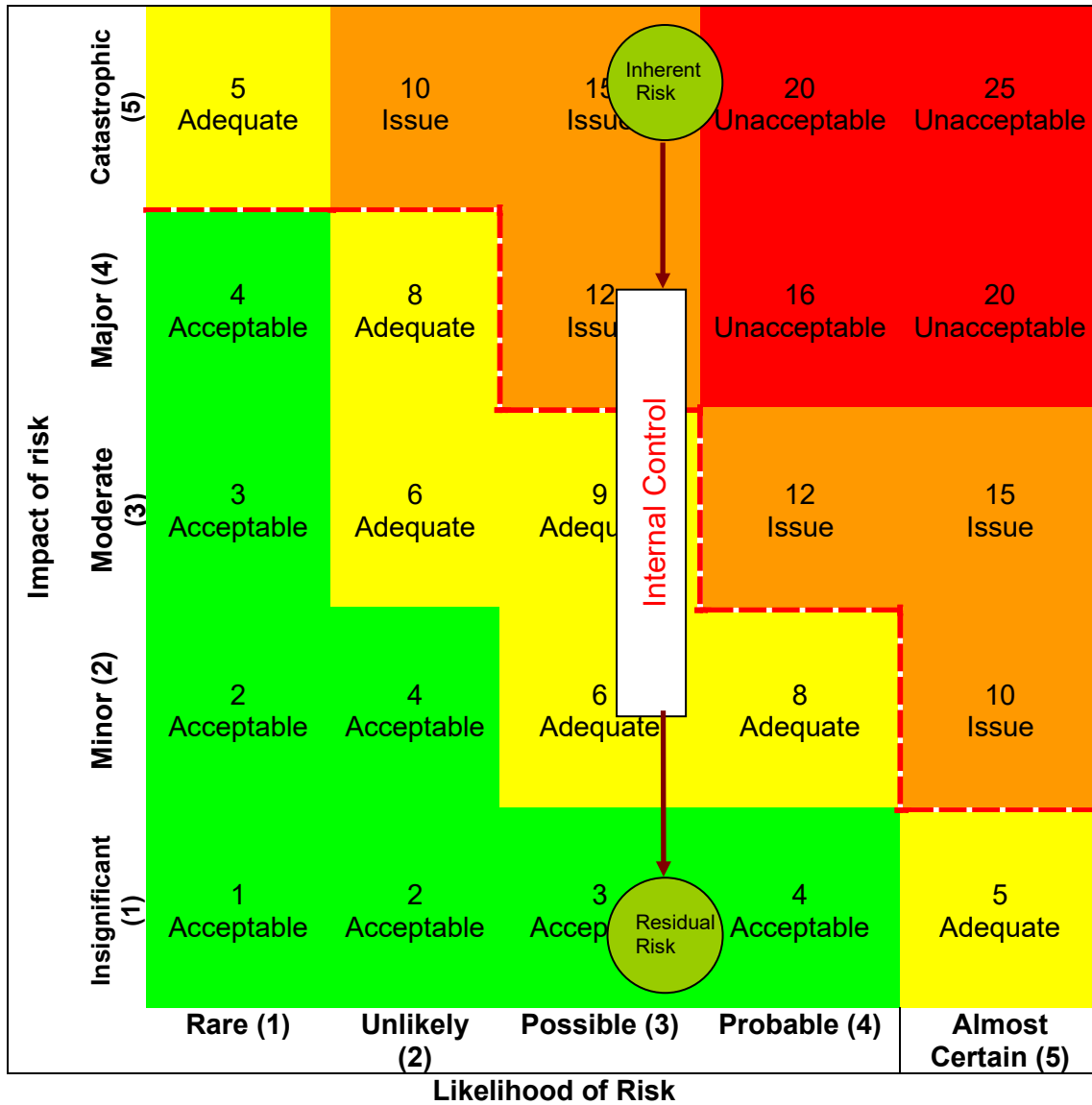
Having used the tables above to score the inherent risk (ie the risk before any corrective action is applied), the next step is to plot the inherent risks on the matrix as shown below.

<b>Impact of risk</b>	<b>Catastrophic (5)</b>	5 Adequate	10 Issue	15 Issue	20 Unacceptable	25 Unacceptable
	<b>Major (4)</b>	4 Acceptable	8 Adequate	12 Issue	16 Unacceptable	20 Unacceptable
	<b>Moderate (3)</b>	3 Acceptable	6 Adequate	9 Adequate	12 Issue	15 Issue
	<b>Minor (2)</b>	2 Acceptable	4 Acceptable	6 Adequate	8 Adequate	10 Issue
	<b>Insignificant (1)</b>	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Adequate
		<b>Rare (1)</b>	<b>Unlikely (2)</b>	<b>Possible (3)</b>	<b>Probable (4)</b>	<b>Almost Certain (5)</b>
<b>Likelihood of Risk</b>						

### 3 Assessment and Prioritisation of Risk (Continued)

Having carried out the inherent risk assessment, the next task is to establish what control procedures exist. These could include policies, protocols, regular meetings or any other activity that has the effect of controlling the identified risk. Once the control measures are identified and validated, a second risk assessment should be performed, again using the Likelihood and Impact criteria but this time taking account of the known control measures. The result of this second assessment is the “Residual Risk”.

The table below shows the matrix discussed previously with colour coding to indicate levels of prioritisation.



Risk Appetite - The boundary between the acceptable risks and those which require managing

### 3 Assessment and Prioritisation of Risk (Continued)

An explanation of the risk scores and how the risk should be managed is as follows:

Level of Risk (Inherent Risk Score)	Indicated by	How risk should be managed
Very High Risk (16-25)	<b>Red</b>	<b>Requires active management.</b> High impact/high likelihood: risk requires active management to manage down and maintain exposure at an acceptable level.
High Risk (10-15)	<b>Amber</b>	<b>Contingency plans.</b> A robust contingency plan may suffice together with early warning mechanisms to detect any deviation from plan.
Medium Risk (5-9)	<b>Yellow</b>	<b>Good Housekeeping.</b> May require some risk mitigation to reduce likelihood if this can be done cost effectively, but good housekeeping to ensure the impact remains low should be adequate. Reassess frequently to ensure conditions remain the same.
Low Risk (1-4)	<b>Green</b>	<b>Review periodically.</b> Risks are unlikely to require mitigating actions but status should be reviewed frequently to ensure conditions have not changed.

### 4 Management and Control of Risk

We now need to consider what action is needed to manage the residual risks. The main options for addressing residual risk are set out in the following table:

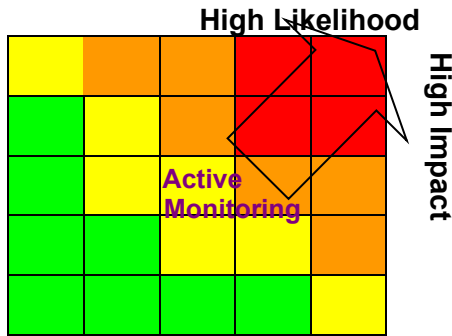
#### 4 Management and Control of Risk (Continued)

<b>Tolerate</b>	<p>Is the exposure tolerable without any further action being taken? Even if it is not tolerable, the ability to do anything about the risk may be limited or the cost may not be proportionate to the potential benefit gained. This option may be supplemented by contingency planning for handling the impacts that will arise if the risk is realised.</p>
<b>Treat</b>	<p>The greatest number of risks will be addressed in this way. While continuing the activity that gives rise to the risk, action is taken to limit the risk to an acceptable level.</p> <p>Where the decision is to treat the risk, mitigating actions need to be defined. It is important that any additional action is proportionate to the risk. Apart from the most extreme undesirable outcome, it is normally sufficient to design controls to give a reasonable assurance of confining any loss to a level that is acceptable to the Council. Each control action has an associated cost and it is important that the control action offers value for money in relation to the risk that it is controlling.</p>
<b>Transfer</b>	<p>For some risks, the best response may be to transfer them. This might be done by insurance or by paying a third party to take the risk in another way. This may be considered appropriate as it reduces the risk to the organisation or because another organisation is more capable of managing the risk.</p>
<b>Terminate</b>	<p>Some risks will only be treatable to acceptable levels by terminating the activity. There may be limited opportunities for the Council as the activity is driven by legislative requirements.</p>

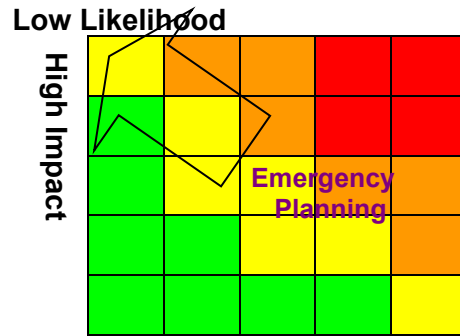
## 5 Review and Reporting

It is important that the management of risk is reviewed and reported on a regular basis in order to monitor whether or not the risk profile is changing and to gain assurance that risk management is effective and to identify when further action is necessary.

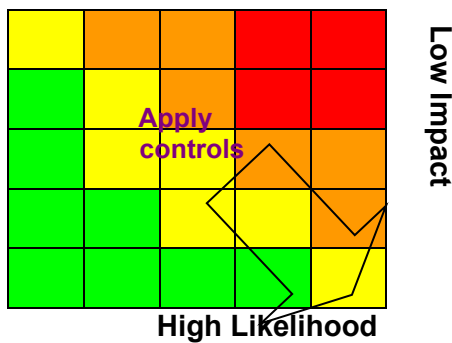
Risks should be monitored according to the following criteria:



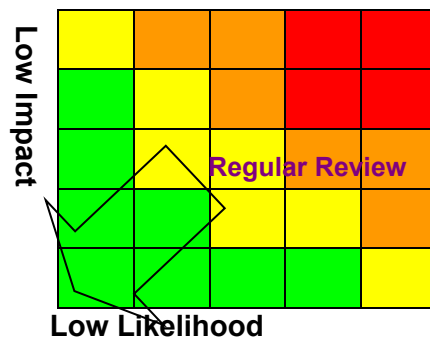
**High impact and highly likely risks which must be managed effectively.**



**High Impact but not likely given either the controls in place or the nature of the risk. Management should periodically review controls and contingencies to deal with these risks.**



**Low impact and low likelihood risks which should be reassessed on an annual basis to ensure their impact and likelihood does not increase over time.**



The Audit Committee is the responsible committee for ensuring that the Council's risk management arrangements are effective and operate as intended.

The Audit Committee will receive regular reports on risk management from the Head of Legal, Democratic, Digital & Customers Services.