APPENDIX A

RISK MANAGEMENT POLICY & FRAMEWORK

Our policy is to identify, analyse and manage potential threats and opportunities posed by risk.

Peterborough City Council (PCC)
2024 -2025

RISK MANAGEMENT POLICY STATEMENT

Risk (and this is defined later in the strategy) is an integral part of everything we do in the Council, inextricably linked to the achievement of our Strategic Aims, Objectives, Priorities and Values. In fact, effective, robust, and proportionate risk management can provide greater assurance as to the achievement of objectives at all levels, including for individuals, that, in turn, ensures the Council can move forward and develop. Pro-active risk management ensures the Council not only meet current needs, including those of the Community, but also ensures it can meet the challenges of tomorrow.

The management of risk is an essential component part of performance management and if robust, proportionate, and embedded, represents excellent Council governance. For risk management to be successfully embedded, we will ensure strong leadership, accountability, learning and sustained communication in all directions and involving all internal and external staff, partners, and stakeholders, who will have differing needs and expectations.

The Council will be open and transparent about the risks it faces and ensure that adequate and robust controls are in place to manage and mitigate risks in accordance with the Council's Risk Appetite (more detail is provided later in the framework). In terms of adopting a proportionate approach, the level of controls must provide adequate protection from the identified risks, but without stifling opportunities for development and enhancement.

Formally incorporating risk management into the day-to-day business of the Council increases focus on what needs to be done (and in fact not done) to meet objectives and at all levels and improve performance.

The Council's members and the Corporate Leadership Team (CLT) are firmly and unequivocally supportive of risk and the risk management process, embedding a risk management culture across all levels of the Council and ensuring the integration of risk management techniques in the decision making process, planning processes at all levels, including from the top down, strategically, and also to raise the general level of awareness and understanding of risk as a concept and in doing so enhancing risk capability and capacity across the Council.

This Risk Management Framework sets out to provide easy to follow guidance on the identification and management of risk at all levels.

SIGNED:

Chief Executive of Peterborough City Council

SIGNED:

Leader of Peterborough City Council

SIGNED:

Deputy Leader and Cabinet Member
for Corporate Governance and Finance

Purpose:

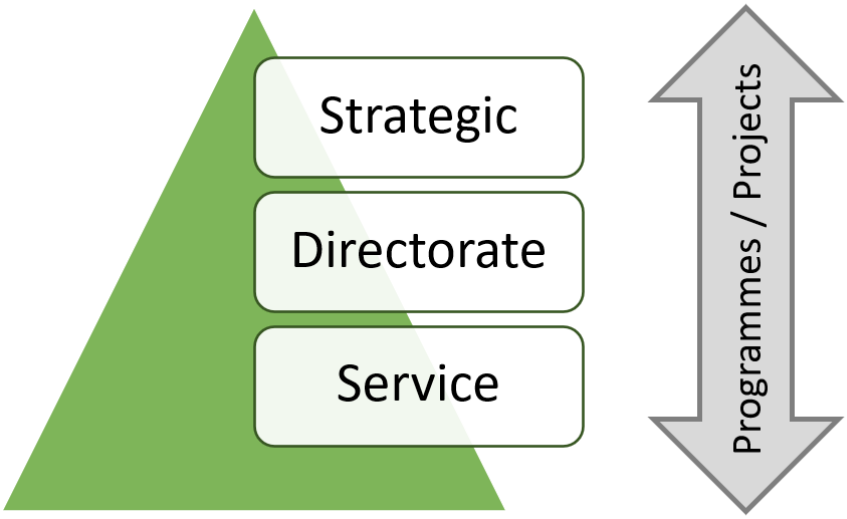
The purpose of this framework is to explain our approach and outline the principles of risk management, identify the people responsible for it, and promote a culture of risk management throughout the Council. This document forms one part of our risk management framework.

Effective Risk Management is a key part of our approach to assuring the Council's performance. Risks on the Council's Risk Registers and our Key Performance Indicators are regularly cross-referenced to ensure our performance improvement actions address any emerging risks. This document has been developed alongside the emerging Performance & Improvement Framework.

Individual members of the Corporate Leadership Team (CLT) are responsible for the Council's strategic risks, and these are reviewed and updated regularly in consultation with the Risk Manager. In exceptional circumstances, issues are also recorded on the strategic risk register.

Directorate level risks are owned by Executive Directors, Directors or Heads of Service and are discussed and reviewed at Directorate Management Team (DMT) meetings.

Most of our risks are service level risks which are owned by an appropriate person, usually a manager or Head of Service, with specialist knowledge of the subject.



Program or Project risks can exist at any level and within any service and should be managed using the same risk management process as other risks.

It should be noted that some risks are outside of the authority's control; this is especially true in a Local Government setting where statutory requirements need to be fulfilled. Whilst it is accepted that it may not be possible to prevent such risks occurring, it is expected that contingency plans/strategies are put in place to minimize / plan for any impact.

Definition of Risk:

There are unlimited definitions of risk as a concept, but the following are good examples:

- Represents the potential for losing something (or indeed gaining something)
- Represents uncertainty, unpredictability, or an event or condition that if it happens or occurs might have a negative impact on the achievement of objectives (at any level)
- Represents a threat but also an opportunity of a positive outcome.

Definition of an Issue:

Whilst this framework focuses on the Management of Risk, Issues Management also needs to be defined. Again, there are numerous definitions. An Issue is an event or sequence of events that has occurred or has happened. In a sense, an Issue is a Risk that has materialized or been exposed. This might conceivably have happened if Risk Management has not been adequate or sufficient despite the best of efforts. The Risk Management framework and strategy requires Risks to be escalated when a particular threshold/score has been reached and then be formally managed accordingly and receive a higher level of attention.

Other criteria that might determine the escalation of a Risk are:

- Risk Treatment required exceeds the authority or mandate of the designated Risk Owner.
- Risk Treatment required the commitment of expenditure beyond the Risk Owner's Authorization Limits.
- Risk cuts across several or may impact negatively on several different risk categories, such as Reputation, Regulatory, Financial, Staffing, Stakeholders and Data/Information/AI for example.

HMT Principles of Risk Management:

The Risk Management framework supports the consistent and robust identification and management of risks and opportunities across the different levels of the Council. For the management framework to be effective, several key principles should be observed.

The Treasury (HMT) Orange Book (2023) sets out the key principles of Risk Management as follows:

- "Risk Management shall be an essential part of Governance and Leadership and fundamental to how the organisation is directed, managed, and controlled at all levels.
- Risk Management shall be an integral part of all organisational activities to support decision making in achieving objectives.
- Risk Management shall be collaborative and informed by the best available information and expertise.
- Risk Management processes shall be structured to include Risk Identification and Assessment to determine and prioritise how the risks should be managed, the selection, design and implementation of Risk Treatment options (more detail is given later in framework), that support achievement of intended outcomes and manage risks to an acceptable level (determined by the Risk Appetite, more detail later), the design and operation of insightful and informative Risk Monitoring and timely, accurate and useful risk reporting to enhance the quality of decision making and to support management and oversight bodies in meeting their responsibilities.
- Risk Management shall be continually improved through learning and experience".

Additional Principles of Risk Management:

To these principles, the Council considers the following are also appropriate and will be applied:

- Behaving with integrity, demonstrating strong commitment to Council published Values, including Ethical Values and in respecting the rule of law.
- Ensuring openness, honesty, and sustained internal and external stakeholder engagement.
- Defining priority outcomes in terms of sustainable, economic, social, and environmental benefits.
- Determining the interventions necessary to optimise the achievement of the intended priority outcomes.
- Developing the Council's capacity, through the capability of its leadership and the individuals within it.
- To incorporate, embed and integrate Risk Management with all Council business from strategic planning, planning at all levels.
- Sharing good practices to assist in continuous improvement and development of the Council as an excellent business.
- Not only managing Risks but also Performance through robust, proportionate internal controls and strong public financial management.

Council Risk Management Objectives:

The Council's key Risk Management objectives are as follows:

- To integrate and embed Risk Management into the culture of the Council.
- To manage Risks (and Issues) in accordance with a sound governance framework (see below).
- To anticipate, respond and be pro-active to change, specifically changing economic, political, environmental, social, legislative, and technological requirements.
- To prevent injury, damage, and losses, including through robust safeguarding measures through robust risk management.
- To promote, openness and transparency as core Values as standard business practice.
- To raise awareness of the need, the principles, and benefits of Risk Management by all those connected and involved in the delivery of Council services.
- To manage business risks, at Strategic, Directorate, Service and Portfolio levels not only as part of Business-as-Usual (BAU) but also as part of our ongoing Transformation Project and Improvement Programmes contained therein.

Achievement of Objectives:

These objectives will be achieved as follows:

- Establishing and clearly defining Roles, Responsibilities and Accountabilities within the Council for those responsible for Risk and Issues Management. (**Appendix A**)
- Incorporating Risk Management considerations into all levels of Business Planning and Service Delivery.
- Providing opportunities for Shared Learning including E-Learning (through the My Learning on-line training facility and including the development of Risk Awareness Workshops and Presentations to internal and external stakeholders.
- Delivering a Framework that allocates resources to meet identified priority risk areas.
- Reinforcing the importance of effective, robust, sustained but proportionate risk management and internal control systems, as part of everyday life and BAU.
- Monitoring the delivery of Risk Management Strategy and Objectives on an ongoing basis.

Benefits of Risk Management:

There are many benefits to the application of Risk Management and Framework, through the adoption of the principles outlined above including:

- Enhanced Performance Management
- Enhanced Delivery of Services
- Greater Assurance that Objectives will be Achieved.
- Enhanced Reputation
- Enhanced Decision-Making at all levels
- Increased Risk Management Capacity and Capability
- More Contented and Stable Workforce
- Stakeholders content/happy with Service Provision
- Enhanced Control over Portfolios, Finance, ICT, Procurement and Contracting and Programmes and Projects and other Generic Risk Areas (See More Detail later).
- Greater Assurance that Transformation Project will achieve objectives.

Risk Management Framework:

Risk Management is not a new process, it does not have to be onerous and get in the way of delivering BAU and Transformation required to ensure the Council operates even more efficiently and effectively. It is a formalization of processes that are already in place but need to be given greater visibility and ensure an even better level of awareness and understanding. Risk Management is integral to a well-managed Council, and it is something that those charged with responsibility for Risk Management should in fact do every day. The Council is committed to embedding Risk Management from the top-down, strategic/corporate level, through all levels of the organization.

Risk Appetite:

The Risk Appetite is the level or amount of risk the Council is willing to take, accept or retain in pursuit of its objectives, at all levels, but starting from the top at Strategic level and before action is deemed to be necessary to reduce the identified risk. Risk Appetite can also be described as the organization's risk capacity, or the maximum or optimum amount of residual (as opposed to inherent) risk it will be prepared to accept after controls and other measures have been put in place. A Risk Appetite statement should address the implications of current strategies and practices.

Factors that influence the setting of the Risk Appetite include:

- The Risk Culture of the Organisation
- The Industry the Organisation sits within
- Competitors
- Types of Initiatives pursued.
- Financial Strength or Resilience of the Organisation

Currently the Risk Appetite as set by the Cabinet is fifteen (15) (following assessment of likelihood and impact considerations).

Risks need to be considered in terms of both opportunities and threats and are not usually confined to money they will invariably also impact on the capability of your organisation, its performance, and its reputation.

Our risk appetite guides how much risk we are willing to seek or accept to achieve our objectives. We recognise we will need to take risks, both in our ordinary business and to achieve the priorities set out in our Strategic Plan.

Good risk management ensures we make well informed decisions, and we understand the associated risks. By ensuring that we properly respond to risks we will be more likely to achieve our priorities. It also provides control and a high level of due diligence consistent with our responsibilities in managing public money.

We recognise effective risk management considers not just threats but also opportunities. So, our approach to risk is to seek the right opportunities and, where possible, minimise threats. By encouraging managed risk taking and considering all the available options we seek a balance between caution and innovation.

Our risk appetite reflects our current position; encouraging managed risk taking for minor to moderate level risks but controlling more closely those risks that come further up the scale. Our appetite for risk will vary over time depending on our ambitions and priorities and the environment we work in, and we recognise that the council provides a wide range of services and therefore, a degree of considered flexibility may need to be applied where appropriate.

The Risk Management Process:

The Risk Management Process includes the following steps:

- Risk Identification including Opportunities.
- Risk Assessment and Prioritisation.
- Risk Treatment/Management (see various available treatments below).
- Risk Registration/Documentation
- Risk Review and Monitoring
- Risk Reporting and Evaluation.

Risk Identification:

The first and most important part of the Risk Management process is the identification of risk. Risk should not always be viewed as a negative entity, although largely when referring to risk, we are thinking about the threats to something being achieved, what is going to stop this happening. In terms of what is going to be achieved, these can be (priority) outcomes, outputs, objectives, and benefits. These measures are, for example, what should be in place in relation to portfolios of programs and projects and are worth highlighting because these play a large part in the delivery of Council BAU and Transformation. Another approach would be to identify risks to the achievement of Strategic, Directorate and Service objectives. The Transformation Project has required the identification of risks to Service Delivery Plans (SDPs). Care should be taken to identify the risk accurately (obvious perhaps), but sometimes the risk is identified as the consequence of the risk (event) occurring/happening, rather than the risk itself. The best approach is to identify the risk and the outcome or consequence of exposure, for example “Failure to remain financially resilient in the face of internal and external pressures leading/resulting in inability to achieve strategic objectives”.

There are many ways of identifying risks including:

- Skills and Experience of the concept of Risk.
- Service Reviews including Delivery.
- Risk Workshops for example at Strategic, Directorate and Service levels.
- Current Internal Controls in place and more importantly operating effectively (or not).
- Change for example in Legislative, Technological or Political environments.
- Review of Performance Indicators and Management Information.
- Insurance Claims or Loss of Data or Breaches in Data Requirements

Categorizations of Risks:

The above trigger list includes some specific Risk Groupings. Others are detailed below, with more comprehensive analysis detailed later in the framework. These groupings are common to most organizations and are therefore somewhat generic, but nevertheless important to highlight: (**Appendix B**)

- Strategic
- Reputational
- Legislative/Statutory/Regulatory
- Financial
- Professional/Staffing/Resourcing

- Social
- Economic
- Environmental
- Political
- Technological
- Data/Information/AI
- Portfolio/Program and Project
- Procurement and Contracting (Commercial/Supplier)
- Stakeholder/Customer/Citizen
- Competitive
- Probity
- Physical

Risk Assessment and Prioritization:

Once identified correctly, the defined risk needs to be analysed to assess how serious a threat it poses to the Council. The most common way of doing this is to assess the Impact and Likelihood of the Risk in question, using the above categorizations as listed above in relation to the approved Risk Appetite and the 5 x 5 risk matrix currently being used by the council, with the score determined by multiplying the 'likelihood' score with the 'impact' score. We have adopted this approach as it encourages a decision to be made about whether a likelihood or impact is high or low. It is important to clarify that both Reputational and Financial assessment are not part of the 5x5 assessment process, although they are both captured when assessing the impact should the risk materialize so as to enhance the overall decision-making process. A full descriptive guide to Likelihood and Impact can be seen in **(Appendix C)**

PCC Risk Matrix

LIKELIHOOD						
	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
		1	2	3	4	5

IMPACT

The first assessment of risk produces an inherent risk rating, known as the **R**ed, **A**mber, **G**reen (RAG) rating, produces the **Prioritization** of the Risk in question, prior to treatment of the said risk. Potential available treatment options are listed below, which when applied and assessed will produce the residual risk rating. The most common choice is in the form of **Risk Mitigation.**

Management of Risk – through Mitigation:

We are at the stage of the process where the risk has been identified, assessed, and prioritized and that has produced an inherent risk rating (a risk score based on impact and likelihood considerations as detailed above). The approved Risk Appetite (by the Cabinet) will also provide a guidance as to the severity of the risk.

Mitigation of risk is the most usual way of managing the risk in question. To ensure a visible ad complete audit trail, the rationale for adopting Risk Mitigation as the preferred approach should be clearly documented.

Responsibility for the risk mitigation should be clearly assigned to an individual with appropriate level of skills and experience, and they are known as the Risk Owner. In some organisations, responsibility for the management of the risk is assigned to a Risk Manager with the nominated Risk Owner assuming overall accountability for the risk in question.

The most common methodology of mitigating risks is through the establishment of internal controls. It is not sufficient to merely put the controls in place, but there need to be systems to ensure said controls are operating as intended. The effective operation of controls should hopefully reduce the Inherent risk score or rating to a residual risk score or rating, or target rating. If not, this might indicate that mitigations are not working and alternative ways to reduce the risk need to be considered.

Types of Internal Controls:

Preventative: Most commonly ensuring adequate segregation of duties to address possible collusion and fraud. Setting and publicizing Financial Authorization/Approval Limits/Levels or restricting access levels to IT systems and data.
Detective: Most commonly Quality Checks or Assurance, Exception Reports, Financial Reports, Project Output Reports that might indicate early warning signs of slippage from timeframes, or worse still, potential project failure.
Directive: Formalized strategies, policies, procedures, training, and guidance form part of an effective Governance Framework. And Systems to monitor compliance especially with Regulatory requirements where failure to comply carries a potentially serious reputational risk.
Corrective: Mitigates the impact through correcting the effects of an event, such as BCP and disaster recovery sites.

And because there is a heavy emphasis on the effective leadership, management and delivery of **Portfolios, Programs and Projects** the following controls should be noted.

- Clearly defined Roles and Responsibilities for Portfolio Director, Program / Senior Responsible Owners (SRO) and Project Managers.
- Appropriately skilled and experienced personnel assigned to these key roles.
- Clearly defined Outputs, Outcomes, Objectives and Benefits and systems in place to measure, achievement.
- Accurate, valid, timely and authorised data and information to measure achievement of project deliverables as above and to assist decision making.
- Risk Management to be carried out from the outset of the task to arrive at an inherent risk score, and then the residual risk remaining after controls have been identified and assessed.

- Acknowledgement that benefits are not necessarily immediately able to be realised so medium-longer term scrutiny is necessary.

- Ability to recognise early warning signs of slippage or potential task failure and courage to stop a failing task.

- Formal undertaking of Lessons Learnt to assist Continuous Improvement.

Registration/Documentation of Risks:

The POWA project management system is used to register, record, and enable monitoring and review of risks through the Power BI front end. As far as this system is concerned, a standard report template has been set up, although a user licence must be formally granted. It provides the facility to produce customised reports to assist risk reporting. We are however currently exploring alternatives to this system and hope to be able to agree a way forward shortly.

Use of Spreadsheets as Risk Registers:

Currently, in addition to the use of POWA, the use of Excel spreadsheets and Word templates to record, register and review risks are commonly used across the Council at various levels. Whilst it is perhaps not ideal to have two systems in operation, rather than one version of the truth, it is perhaps not necessary to be overly prescriptive in these respects until further analysis has been done, which is currently ongoing. But to ensure effective, efficient, and quality reporting there will need to be only one system in use throughout the Council moving forward and will need to include the following component parts.

- Risk Description
- Date Risk Identified
- Risk Owner
- Risk Manager
- Inherent Impact Score
- Inherent Likelihood Score
- Inherent RAG Rating
- Proposed Mitigations
- Target Residual Score – Still under consideration
- Actual Residual Impact Score
- Actual Residual Likelihood Score
- Actual Residual RAG Score
- Trend (Decreasing-Stable-Increasing)
- Comments

Assurance and the Three Lines of Defence:

Checks caried out by those charged with responsibility for Risk Management form part of the organizations' Three Lines of Defence Assurance Framework, that includes Internal Audit who provide their independent and objective review of the effectiveness of Internal Controls and Risk Management as part of their standard remit, the Three Lines of Defence model is explained in greater detail. (**Appendix D**)

Monitoring and Review of Risks:

Monitoring and review of risks should form part of BAU and be embedded within the culture of the Council and supported by the Corporate Risk Manager. It is not enough to identify risks and then put them to one side. They

should be monitored and reviewed regularly. Reviews should of course include representation by the designated Risk Owner but there will other relevant contributors at Strategic, Directorate and Service levels. Risk reviews will also form part of key projects such as the Transformation Project and the Decoupling Project. There is no definitive period of elapsed time from one review to another but suffice to say and depending on the severity of the risk and the RAG rating assigned (following assessment and prioritization) that too much rather than too little is probably the preferable strategy, so for example at each DMT or each Portfolio Board (PB) meeting, risk should be a standard Agenda item.

Rationale for and Scope of Risk and Control Reviews:

There are a range of reasons to review identified risks. Here are ten (10) examples:

- Are mitigations working, having their desired effect?
- Should risks be classified as opportunities as opposed to risks?
- Do controls have to be strengthened or adapted?
- Are mitigations decreasing, increasing, or stabilising in terms of trend?
- Are there any risks that need to be escalated to become Issues (See Triggers for Escalation)
- Are there any new risks to the achievement of objectives, for example resultant from new or changing legislation?
- Are there any risks that have been mitigated and can be considered as being closed?
- Are the risks still valid or do impact and likelihood scorings suggest they are not risks?
- Is responsibility for ownership of the risk assigned to the correct entity, for example at Service level, or Directorate level?
- Are changing service or stakeholder demands meaning the risk needs to be revisited?

Risk Reporting:

There are several existing sources and mechanisms to report risk as follows:

- Via Portfolio Boards (PB) of which there are four (4) re the Transformation Project
- Via Directorate Management Teams (DMTs) & Service Delivery Teams
- Via the Risk Management Board (RMB) which meets Bi- Monthly and accepts risk reports from members from within Directorates and Service Delivery Teams, ensures escalation of risks (see below) and that reports potentially new Strategic Risks to the CLT, via the Strategic Risk Register.
- Via the Corporate Leadership Team (CLT) who have monthly meetings to discuss and update the Strategic Risk Register at Performance (PCLT)
- Via the CLT Director or the RMB re Escalation of Risks
- Via the Cabinet and Audit Committee (see below)

It is important that there is a joined-up risk reporting process in place and operating effectively and it is the responsibility of the Council Risk Champion/Co-ordinator to ensure this happens, through invitation and attendance at meetings at the different levels, to ensure a consolidated and consistent reporting process. This will involve careful and considered scheduling of meetings at the different levels, so that, ultimately the CLT and the Audit Committee are in receipt of up-to-date risk data.

A detailed visualisation of the process flow can be seen in **(Appendix E)**

Benefits of a Consolidated, Joined-Up Risk Reporting:

- Risk Management will not be duplicated**.**
- Risks will be managed at the most pertinent, correct level.
- Risks will not be missed or overlooked.
- An established Risk Hierarchy will be established and become known to staff.

Cabinet/Committee Reports:

Cabinet/Committee Reports should give appropriate consideration, to the management of risks. Reports should include:

- A realistic, open, and honest explanation of the potential risks arising from a course of action, decision, strategy or policy, or element of the (business) planning process. It is important that the emergence and identification of risks are transparently communicated and that the challenges and mitigations to manage the risks are not downplayed or not visible.
- Mitigation actions to be taken, at inherent stage, to manage and reduce the assessed impact and likelihood of the identified risk happening, to provide a more accurate target residual risk score.
- An explanation as to how Risks are going to be managed, reviewed, mitigated on an ongoing basis and an understanding of factors that may require escalation to an Issue.

Annual Governance Statement:

The Accounts and Audit Regulations require the Council to produce an AGS alongside its Statement of Accounts in each financial year. The AGS is a statutory document which explains the processes and procedures in place to enable the Council to carry out its functions effectively.
Ownership of the document is through CLT. The report sets out progress on previous actions as well as future proposals for ongoing updates.

The AGS is produced following a review of the Councils governance arrangements. The review requires the systems and processes of corporate governance are brought together and reviewed.

- The Local Code of Governance which stands as the overall statement of the Council's corporate governance principles and commitments document is reviewed (Legal)
- An Annual self-assessment by Heads of Service / Executive Directors (no change). Results are shared with CLT recognising that the process of preparing the AGS should, itself, add value to the effectiveness of the corporate governance and internal control framework.
- A separate "Governance Management Group" lead by the Director for Legal and Governance (Monitoring Officer) meet to discuss and identify emerging governance issues and to produce the draft AGS. This should comprise of key Senior Officers with responsibility for governance – namely from Legal, Finance, Risk Management, Audit, Information Governance and Human Resources. This Group reflects CIPFA / Solace guidance whereby "authorities should nominate an individual / group with appropriate knowledge, expertise and levels of seniority to evaluate the assurances and supporting evidence provided to draft the AGS".
- Once the above document has been drafted, it will enable the Chief Internal Auditor the opportunity to review / audit the AGS and to establish whether assurance can be placed on the draft AGS.

The Governance Statement needs to be approved and signed off in a timely manner by the Leader of the Council and the Council Chief Executive.

Within the Annual Governance assurance process, the Chief Executive on behalf of the Corporate Leadership Team (CLT) will be asked to confirm that the Risk Management Framework is embedded, and the principles are being actively applied, within all areas of Council activity and business.

Evaluation Arrangements – How to Measure the Success of the Risk Management Framework:

Just as it is good practice to carry out formal lessons learnt exercises, for example, at the conclusion of projects, at the end of Internal Audits, it is sound business practice to evaluate the success or otherwise of the Risk Management Framework, to ensure continuous improvement and development. So, what might the performance indicators (PIs) be in order to carry out that evaluation, probably somewhat subjective but might include the following measures:

- Risks Effectively Mitigated & Closed
- Achievement of Council Objectives and Priority Outcomes (at all levels)
- Positive Feedback from Stakeholders/Customers/Citizens
- Council Reputation Enhanced
- Council achieves Financial Resilience and Sustainability
- All Regulatory Requirements Met
- Staff Satisfaction Surveys yield positive results.
- Delivery of Transformation Project, all deliverables achieved.
- Delivery of Decoupling Projects all deliverables achieved.
- Enhanced Risk Capability and Capacity
- Positive Outcomes from Internal Audits
- Acceptance of Risk Framework and Reports by Audit Committee
- Strategic Risks Managed and Objectives Achieved
- Directorate & Service Level Risks Managed and Objectives Achieved
- Opportunities identified and taken advantage of through controlled risk taking and optimised positively.

Consideration will be given to the development of specific Performance Indicators (PIs) to ensure the outcomes of the Risk Management Framework can be accurately, appropriately, and clearly measured, if necessary for formal reporting purposes.

Appendix A:

Roles and Responsibilities for Risk Management:

The framework has referred above to the need for clearly defined and allocated Roles, Responsibilities and Accountabilities across the Council as an essential component part of delivering the Risk Management strategy. Below in tabular format are the key roles for delivering the Council Strategy through effective Risk Management as follows:

Risk Management Responsibilities and Accountabilities	
Element	**Expectation**
Cabinet	Consider risk in its strategic planning for the Council. Set and Approve the Risk Appetite for the Council. Monitor performance of management in the treatment of strategic risks including mitigation actions.
Lead member for Risk Management	Champion the operation of effective risk management operations
Audit Committee Scrutiny Committees	Hold Members and Officers to account for effectiveness of risk management in decision making and achievement of objectives.
Corporate Leadership Team (CLT)	Own and lead the strategic risk management process. Own, review and challenge the strategic risk register (SRR). Receive urgent risk reports as necessary.
Lead Director (CLT) for Risk Management (Executive Director of Corporate Services and s151 Officer)	Overall accountability for the effective delivery of the organisation's risk management function including the Strategic Risk Register and the Risk Management Strategy Acts as Sponsor & Attends meetings of Risk Management Board on behalf of CLT.
Directorate Management Teams (DMTs)	Manage Risks at Directorate level and report to Risk Management Board
Heads of Service (HoS) Managers	Manage Risks at Service level and report to Directorate Management Teams and Risk Management Board

Risk Management Responsibilities and Accountabilities	
Element	**Expectation**
Risk Management Board (RMB) – chaired by the Corporate Risk Manager, and (made up of Departmental Risk Co-Ordinator's)	Undertake a regular review of the Risk Register Engage in bi-monthly monitoring and discussion of BAU risk, new operational risk and issues within departments. Coordinate risks in relation to cross-departmental dependencies / crossovers. Consider the success of mitigating strategies. Establish trends for risks including those increasing in severity. Discuss the overall level of threat, and items for escalation to the CLT.
Departmental Risk Co-Ordinator's (Risk Management Board members)	Support and facilitate risk management across their specified area. Act as a champion / coordinator for risk management within their department by providing support to Directors, Heads of Service and other managers on the management of their risks. Regularly table departmental register at DMT's for discussion / refresh Attend Risk Management Risk Board to report on the key risk items. Maintain the departmental risk register.
Portfolio, Program and Project Managers Strategic Programs Lead (Supported by Corporate Delivery Unit)	Ensure that a unified and consistent approach to Project and Program Risk Management covering the identification, recording, monitoring, and mitigation of risks, including Risks relating to the Transformation Project Portfolio. Support in the identification of cross-program risks (and trends) which may become strategic risks. Actively manage risks and issues using resources and approaches within his/her delegates authority - maintain the Program Risk and Issue Registers, Escalate to the SRO recommendations for risk mitigations actions outside the scope of her/his delegated authority, Management and delivery of Portfolios, Programs and Projects as part of BAU, including the Decoupling Project Management and delivery of Improvement Programs and Projects as part of the Transformation Project

Risk Management Responsibilities and Accountabilities	
Element	**Expectation**
Officers / Employees	Manage risk as part of their role and report risks to their managers. Develop understanding of risk management at the Council through completion of e-learning and attendance at any training required.
Chief Internal Auditor (CIA) and Internal Audit (IA)	Current lead officer on development and delivery of the annual audit Risk Based Program of work as approved by the Audit Committee. Routine overview of risk management arrangements through all audit activities.
Corporate Risk Manager	Acts as a Champion for Risk Management across the Council. Development of the Council Risk Management Strategy and supporting Framework. Development and review of the Terms of Reference (TORs) for the Risk Management Board and Chair the meeting. Develops E-learning and other Risk Training materials, develops and delivers Risk Awareness Workshops for both Officers and Members**. (Appendix F)** Attends meetings at DMT and Service levels when required. Provides Risk Reports to the Audit Committee. Conducts Risk and Control reviews.

Appendix B:

Risk Category	Some Descriptions of Risks
Strategic	Strategic Plan not in place or reviewed regularly to ensure continued relevance, and outcomes do not reflect current priorities. No linkage with Strategic Risks identified.
Reputational	Reputation damaged from numerous potential sources, including external stakeholders/customers through failure to deliver services to standards and meet statutory requirements such as those relating to Adult Social Care, Children's Education, Safeguarding. Failure to deliver an environment where people want to live, visit, invest in, due to failure to transform City Centre, for example.
Legislative/Statutory/Regulatory	(See Linkage Above to Reputational Risk). Preparedness and systems to deal with either new legislation or changes to existing legislation, like Waste Disposal. Other legislation might be relating to European Law, Disability Discrimination Act, Section 17 Crime and Disorder Act, Data Protection and Freedom of Information, Human Rights and Equal Opportunities, and Health and Safety (H&S). Public Services (Social Values Act 2012), Welfare Reform Act (2012). Local Government Finance Act (2012) which impacts on Council Tax Rebate schemes, for example. Control is Dedicated Resource to cover Regulatory requirements.
Financial	Failure to remain resilient in face of economic crisis, cost-of-living crisis, high inflation, increased costs, for example re Suppliers. Need to utilise reserve budget that may not be adequate. Excessive Insurance Claims. Failure to plan, manage and control budgets.
Professional/Staffing/Resourcing	Right staff not in the right place and time. High turnover due to work pressures. High instances of long-term sickness absence. Recruitment problems in attracting decent quality staff. Failure to attract staff into hard to fill vacancies or specialist roles.
Social	Demand for school places not met by supply. Childcare Availability – Demands not met and Costs Prohibitive Equality Analysis regarding Age, Disability, Gender, Religion, Race and Sexual Orientation. Leisure and culture provision not meeting needs. Increase in crime and criminal activity. Housing/residential needs not met increasing homelessness.
Economic	High Inflation, High interest Rates Increased Energy Costs Cost-of-Living Crisis Increased Supplier Costs Property Prices – Affordable Housing
Environmental	Waste Disposal and Recycling Pollution – Air Quality Traffic Congestion Extreme Weather – Climate Change
Political	Change of Council Leadership – Hung Council Change of Central Government or its Policies Reduced Future Budget Allocations
Technological	Technological change not identified or embraced. Change not managed. Technology not affordable Capacity to deal with e-government targets. Technology Partners – Increased Costs Data Security/Phishing Data Breaches/Losses due to High Staff Turnover

Appendix B Continued:	
Data/Information/AI	Linkage with Compliance with Regulatory Requirements and Issues relating to Technology as above. Potential for AI as an opportunity not identified/realised
Portfolio/Programs/Projects	Outputs, outcomes, objectives, and benefits not defined at the outset, and systems in place to measure achievements not adequate. Risks not identified at the outset. Leadership, management, and delivery not adequately resourced. Data and information to assist effective decision making not adequate. Basis of decisions not documented. Early warning signs of project failure or slippage not acted upon. Mismatch between resource allocations and deliverables. Reputation impacted negatively.
Procurement and Contracting (Commercial/Suppliers)	Procurement practices does not comply with rules and regulations. Single tendering used but not justified. Little focus on SMEs as part of competitive tendering. Focus on cost rather than other criteria (quality and innovation for example). Supplier price increases. Inadequate Contract/Supplier Management. Contracts broken either deliberately, or un-intentionally. Contract wording contain ambiguous requirements. SLAs not achieved. Customer complaints about delivery.
Stakeholder/Customer/Citizen	Stakeholder population not known or fully identified. Needs and requirements of stakeholders/customers/citizens not identified or not met. Poor relationships with stakeholders rather than through adoption of values such as openness and honesty. Needs not met through financial pressures and need to re-prioritise. Complaints potentially harming reputation and credibility. Citizens affected negatively through social, environmental, and economic issues and situations.
Competitive	Lack of knowledge of the competition Lack of competitive spirit Failure to secure contracts in face of competition Poor relationships with competitors build on being adversarial. Performance Indicators (PIs) flawed or other performance data making it problematic to compare performance against competitors.
Probity	Staff shortages or dissatisfaction leading to staff acting in an improper or untrustworthy way.
Physical	Not all assets known including values. Not all assets part-owned/leased not known including financial contribution. Assets not known or identified for disposal. Security and Health and Safety considerations not addressed adequately. Potential hazards such as falling trees, leading to insurance claims. Physical risks relating to or arising from vehicles/transportation, plant, equipment, and machinery. Relevant legislation such as Equalities Legislation and Disability Discrimination Act impacting on accessibility to buildings.

Appendix C

Impact and likelihood definitions

IMPACT	Negligible (1)	Low (2)	Moderate (3)	Significant (4)	Very High (5)
Public and employee health, safety, and wellbeing	None	Minimal level of harm to the health, safety and wellbeing of the community, members of the public or employees	Moderate level of harm to the health, safety and wellbeing of the community, members of the public or employees	Significant level of harm to the health, safety and wellbeing of the community, members of the public or employees	Substantial level of harm to the health, safety and wellbeing of the community, members of the public or employees
Service Disruption	No loss of service	Minimal external or internal disruption and/or loss of service (less than 24 hours)	Moderate external or internal disruption and/or loss of service (between 24 to 48 hours)	Significant external or internal disruption and/or loss of service (between three to seven days)	Substantial external or internal disruption and/or loss of service (more than seven days)
Environmental	None/ Insignificant	Minimal regional environmental damage and/or failure to meet all or most internal climate change targets	Moderate regional environmental damage and/or failure to meet all or most internal climate change targets	Significant regional environmental damage and/or failure to meet all or most internal climate change targets	International and/or national environmental damage
Information Security	No Impact	Minimal external breach with no loss of sensitive data; or minor external breach with loss of sensitive data	Moderate external breach with no loss of sensitive data; or minor external breach with loss of sensitive data	Significant external breach with no loss of sensitive data; or minor external breach with loss of sensitive data	Substantial breach; Information Commissioner Office (ICO) fine; loss of ISO 27001 certification
Skills Capability	No impact	Minimal under performance from skills gaps and/or shortages	Moderate underperformance from skills gaps and/or shortages	Significant underperformance from skills gaps and/or shortages	Substantial underperformance from skills gaps and/or shortages
Community	No impact	Minimal disadvantage to large parts of the community and/or some vulnerable residents	Moderate disadvantage to large parts of the community and/or some vulnerable residents	Significant disadvantage to large parts of the community and/or some vulnerable residents	Substantial disadvantage to large parts of the community and/or many vulnerable residents
Economy	No impact	Minimal negative impact on the County's economy, including hard infrastructure	Moderate negative impact on the County's economy, including hard infrastructure	Significant negative impact on the County's economy, including hard infrastructure	Substantial negative impact on the County's economy, including hard infrastructure
Legal	No impact	Minimal legal action, claims and/or penalties against or by the Council	Moderate legal action, claims and/or penalties against or by the Council	Significant legal action, claims and/or penalties against or by the Council	Substantial legal action, claims and/or and penalties against or by the Council
Contracts and Partnerships	No impact	Minimal impact on service delivery from a contract and/or partnership failure	Moderate impact on service delivery from a contract and/or partnership failure	Significant impact on service delivery from a contract and/or partnership failure	Substantial impact on service delivery from a contract and/or partnership failure

Appendix C cont.

LIKELIHOOD	Negligible (1)	Low (2)	Moderate (3)	Significant (4)	Very High (5)
Definitions	Event could occur every 10 years or longer	Event could occur every five years	Event could occur every two years	Event could occur every year	Event expected to occur every year

Financial impact assessment -

Each risk is assessed for the potential range of capital and/or revenue loss to the Council if the risk materialised.

Band 8 Loss over £20 million
Band 7 Loss between £10 million and £20 million
Band 6 Loss between £5 million and £10 million
Band 5 Loss between £3 million and £5 million
Band 4 Loss between £1 million and £3 million
Band 3 Loss between £100,000 and £1 million
Band 2 Loss between £50,000 and £100,000
Band 1 Loss under £50,000
Band 0 No financial loss

Reputational impact assessed if the risk materialised.

Extremely High - Lasting or permanent national/local brand damage resulting from adverse comments in national press and media. High chance of Councillors/PCC staff forced to resign.
High - National/local brand damage lasting up to two years from coverage in national, regional and/or local press/media. Councillors/PCC staff potentially forced to resign.
Moderate - Temporary local brand damage lasting up to one year from extensive coverage in regional and / or local press/ media.
Low - Temporary local brand damage lasting up to a few weeks may be possible from minor adverse comments in local press/social media.
Extremely Low - Negligible local brand damage from limited adverse comments with minimal press/social media.

Appendix D:

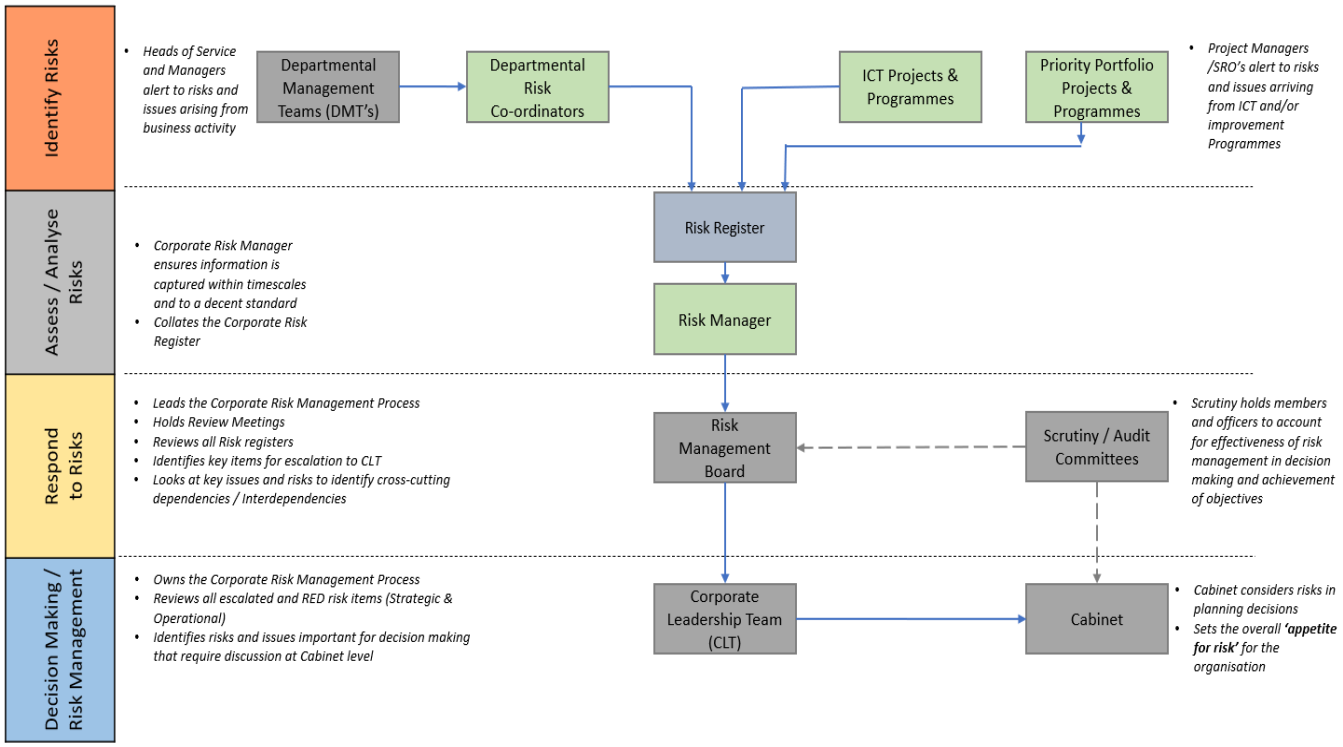
Three Lines of Defence Assurance Model:

First line: (functions that own and manage risks) is formed by managers and staff who are responsible for identifying and managing risk as part of their accountability for achieving objectives. Collectively, they should have the necessary knowledge, skills, information, and authority to operate the relevant policies and procedures of risk control. This requires an understanding of the Council, its objectives, the environment in which it operates, and the risks it faces.

Second line: (functions that oversee or who specialise in compliance or the management of risk) provides the policies, frameworks, tools, techniques, and support to enable risk and compliance to be managed in the first line, conducts monitoring to judge how effectively they are doing it and helps ensure consistency of definitions and measurement of risk.

Third line: (functions that provide independent assurance) is provided by internal audit. Sitting outside the risk management processes of the first two lines of defence, its main roles are to ensure that the first two lines of are operating effectively and advise how they could be improved. Tasked by, and reporting to the Audit Committee, it provides an evaluation, through a risk-based approach, on the effectiveness of governance, risk management, and internal control to the organization's governing body and senior management. It can also give assurance to sector regulators and external auditors that appropriate controls and processes are in place and are operating effectively.

Appendix E – Visualisation of the process flow



Appendix F:

Training and Guidance:

The success of the Risk Management Framework is dependent to an extent on the capability of staff assigned either, direct responsibility as Risk Owners but also other Support Staff. Indeed, key partners within the Framework such as the Audit Committee might conceivably benefit from some form of training. Thinking about the provision of training and guidance is in its infancy at the point of drafting this document but so far, has taken the form of the following:

- Simple Bite-Sized pieces of written guidance. The following have already been prepared.

  Roles and Responsibilities for Risk Management
  Key Principles of Risk Management
  Risk Categorizations
  Risk Management Life Cycle
  Risk Treatment Options
  Benefits of Risk Management
  Definitions of Risk Management
  From Risks to Issues

This framework document already includes information on each of these areas.

- Use of on-line learning materials and functionality currently being explored.

- Development and delivery of Risk Awareness Workshops and Presentations either remotely or in person or a mix of the two also being explored.

- Production of ad hoc guidance for publication on the PCC Intranet facility. A site dedicated to Risk Management has already been established and utilised to convey key messages about the concept of risk and risk management but needs to be reviewed and re-launched.

This page is intentionally left blank