APPENDIX 1 – KCC Risk Management Policy and Strategy 2021-24

1. Statement of Commitment

1.1 The Cabinet and the Corporate Management Team are committed to effective risk management and see it as a key part of KCC's responsibility to deliver effective public services to the communities within Kent.

1.2 There is a shared commitment to embedding risk management throughout the organisation, promoting a positive risk culture and making it a part of everyday service delivery and decision-making, ensuring that sufficient resources are allocated. This includes fostering an environment that embraces openness, supports integrity, objectivity, accountability and transparency in the identification, assessment and management of risks, welcoming constructive challenge and promoting collaboration, consultation and cooperation. We must invite scrutiny and embrace expertise to support decision-making, invest in the necessary capabilities and seek to continually learn from experience.

1.3 By implementing sound management of our risks and the threats and opportunities that flow from them we will be in a stronger position to deliver our organisational objectives, provide improved services to the community, achieve better value for money and demonstrate compliance with the Local Audit and Accounts Regulations. Risk management will therefore be at the heart of our good management practice and corporate governance arrangements.

1.4 Risk management enhances strategic planning and prioritisation, assists in achieving objectives and strengthens the ability to be agile to respond to the challenges faced. To meet our objectives, improve service delivery and achieve value for money for the residents of Kent, risk management must be an essential and integral part of planning and decision-making.

2. Purpose and Scope of the Policy and Strategy

2.1 The aim of this Risk Management Policy and Strategy is to support the delivery of organisational aims and objectives through effective management of risks across the Council's functions and activities, applying appropriate risk management processes, analysis and organisational learning.

2.2 It explains our approach and outlines the principles of risk management, as well as clarifying risk management roles and responsibilities across the council. This document is aligned with the Council's key organisational strategies and plans and is part of our risk management framework.

2.3 This policy applies to all of KCC's core functions. Where KCC enters into partnerships the principles of risk management established by this policy and supporting guidance should be considered as best practice and applied where possible. It is also expected that our significant contractors have risk management arrangements at a similar level, which should be established and monitored through commissioning processes and contract management arrangements.

2.4 This document draws on several sources. This includes the Cabinet Office publication *Management of Risk: Guidance for Practitioners*; the most recent HM Treasury publication *"The Orange Book: Management of Risk – Principles and Concepts";* and is informed by the UK implementation of the international standard for risk management BS *ISO 31000: 2018.*

2.5 There are different but aligned risk management processes that are applied at different levels within the organisation. Risk specialists are embedded across the organisation in areas such as Health and Safety; Treasury Management; Emergency Resilience and Business Continuity; Insurance; Information Security and Governance; Counter-Fraud etc. These specialist risk areas each have their own policies, procedures and processes that are built into the governance arrangements of the council so that work is coordinated within the council's overall risk management framework.

2.6 The Policy and Strategy is supported by a Risk Management Toolkit that guides, supports and assists staff in achieving successful risk management.

3. Risk Definitions

3.1 Risk is defined as, "The effect of uncertainty on objectives. It can be positive, negative or both and can address, create or result in opportunities and threats."

3.2 Risk management is defined as: "Co-ordinated activities to direct and control an organisation with regard to risk."
(BS ISO 31000:2018 Risk Management Guidelines)

4. Risk Management Strategy

4.1 The operating environment for local government has become increasingly challenging over the past decade, in terms of growing and complex service demand, additional statutory requirements and increasing resident expectations, all set against a backdrop of local government funding restraint. This continuing trend requires greater collaboration, system-wide planning and a strong understanding of risk across public services.

4.2 In addition, the coronavirus pandemic and its major social and economic impacts is fundamentally changing the risk environment, with it likely to be even more volatile, complex and ambiguous for a number of years. The risks arising in this environment will often have no simple, definitive solutions and will require whole-system-thinking, aligned incentives, positive relationships and collaboration, alongside relevant technical knowledge, to support multi-disciplinary approaches to their effective management.

4.3 The operating environment will also require the Council to continually review its risk appetite, not only to ensure the right balance is struck between risk, innovation and opportunity, but to consider how much control can be exerted over risks, many of which cannot be directly mitigated by the Council alone.

4.4 In the context of continual and fast-paced change, our elected Members will need to make challenging policy and budgetary decisions, while maintaining a longer-term view, so officers will need to provide the right balance of evidence, insight, advice and understanding of risk and opportunity.

5. Risk Management Objectives

5.1 In support of the Council's governance and internal control arrangements and achievement of KCC's objectives, the Council is committed to:

- Managing risk in accordance with good practice and sound governance principles.
- Embedding effective risk management into the design, values and culture of the council.
- Integrating the identification and management of risk into policy and operational decisions.
- Proactively anticipating and responding to changing social, economic, political, environmental, legislative and technological requirements that may impact on delivery of our objectives.
- Eliminating or reducing negative impacts, disruption and loss from current and emerging events.
- Harnessing risk management to identify opportunities that current and emerging events may present and maximise benefits and outcomes
- Managing risks in line with risk appetite.
- Promoting openness and transparency in risk management processes.
- Raising awareness of the need for risk management by all those connected with the Council's delivery of services.

5.2 KCC will achieve these aims by:

- Integrating risk management practices into the Council's decision making, business planning, performance and management activities, particularly focusing on robust analysis, scrutiny and evaluation of mitigating controls and further actions.

- Utilising available business technology to aid visibility and analysis of key risk information across the organisation, including connectivity between risks.
- Providing a varied risk management training and development offer for both officers and elected Members, as part of KCC's broader Leadership and Management Strategy.
- Embedding risk management arrangements within major change activities across the council and developing an integrated approach to their assurance.
- Reviewing the Council's risk appetite to ensure it remains aligned with strategic objectives, while promoting a wide understanding of how it translates into tolerance levels within service or programme settings.
- Intelligence sharing and collaboration between risk management and assurance disciplines across all Council activities, consolidating ongoing learning, experience and knowledge. This includes ensuring understanding of how each of the "three lines of assurance" contributes to the overall level of assurance required and how these can be best integrated and mutually supportive.
- Operating sound and transparent risk management arrangements with our partners and providers, underpinned by a culture that supports collaboration and the development of trust, ensuring clarity of risk and control ownership and striking a proportionate balance of oversight of partner / provider risks without being over-constrictive.
- Communicating relevant risk messages to the organisation in a timely manner, listening and responding to feedback received.
- Subjecting KCC's risk management arrangements to regular review to determine their continued adequacy and effectiveness.

6. Risk Management Principles and Framework

6.1 As an integral part of our management systems, and through the normal flow of information, our risk management framework harnesses the activities that identify and systematically anticipate and prepare successful responses.

6.2 The framework is designed to support a comprehensive view of the risk profile, aggregated where appropriate, in support of governance and decision-making requirements. It supports the consistent and robust identification and management of risks within desired levels across the organisation, supporting openness, challenge and innovation in the achievement of objectives.

6.3 There are five key principles of risk management that provide the basis on which KCC will manage risk:

A. Governance and Leadership – 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.

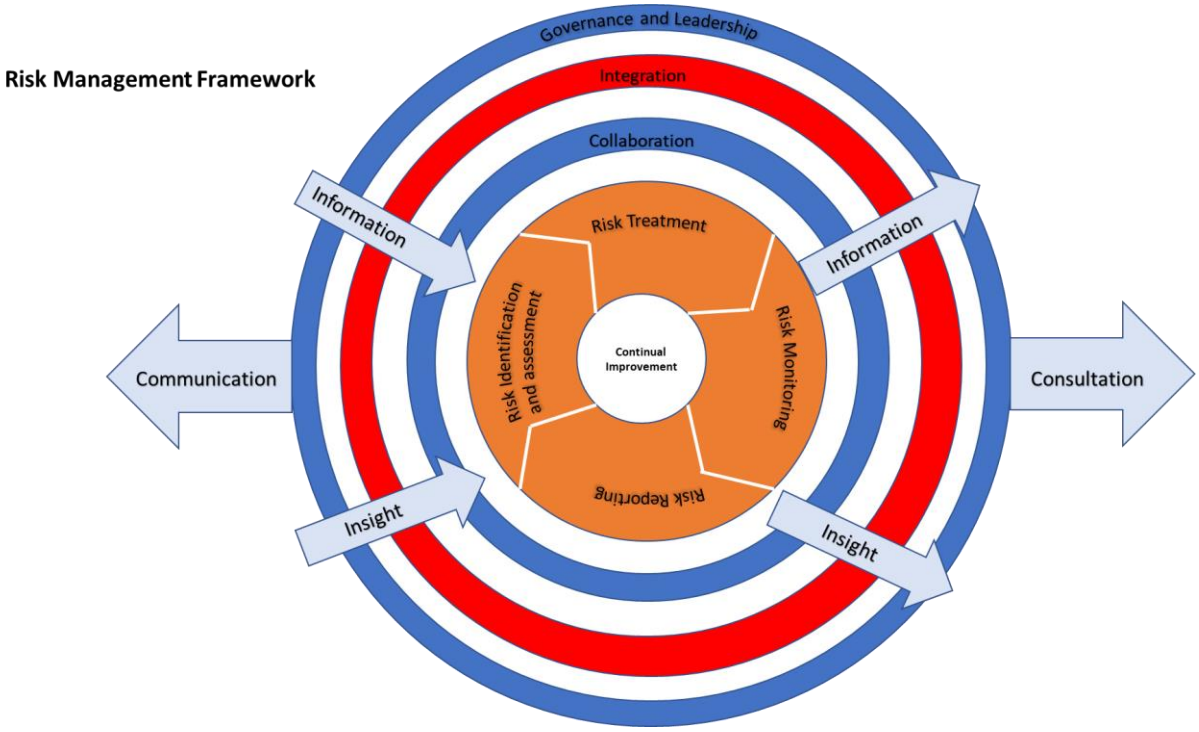
B. Integration – risk management shall be an integral part of all organisational activities to support decision-making in achieving objectives.

C. Collaboration and Best Information – risk management shall be collaborative and informed by the best available information.

D. Structured Processes – risk management processes are recognised as iterative in practice, rather than sequential, and shall be structured to include:

- **Risk Identification and Assessment** – to determine and prioritise how the risks should be managed.
- **Risk Treatment** – the selection, design and implementation of risk treatment options that support achievement of intended outcomes and manage risks to an acceptable level.
- **Risk Monitoring** – the design and operation of integrated, insightful and informative risk monitoring.
- **Risk Reporting** – timely, accurate and useful risk reporting to enhance the quality of decision-making and to support management and oversight bodies in meeting their responsibilities.

E. Continual Improvement – risk management shall be continually improved through learning and experience.



7. Risk Management Processes

Risk Identification and Assessment

7.1 The aim of risk identification is to recognise and articulate the risks that may help or prevent KCC to achieve its objectives. It is particularly relevant to consider new or emerging risks alongside business planning and strategy formulation processes.

7.2 There are several risk perspectives:

Corporate - Those risks, which if they occurred, would have a major impact on the organisation or delivery of its priorities. Corporate risks also include cross-cutting risks that impact across directorates.

Change related (Programme / Project) – where we are exposed to risks that could affect our ability to successfully complete the desired transformational outcomes or deliver predefined outputs that enable us to deliver outcomes and realise benefits.

Operational / Service / Contract – where we are exposed to risks that could affect our control and ability to successfully and continually deliver or commission services to our service users / residents.

7.3 The following factors, and the relationship between these factors, should be considered when identifying risks:

- Changes in the external and internal context
- Causes and events
- Consequences and their impact on objectives
- Threats and opportunities
- Vulnerabilities and capabilities
- Uncertainties and assumptions within options, strategies, plans or initiatives
- Indicators of emerging risks
- Limitations of knowledge and reliability of information
- Time-related factors
- Any potential biases and beliefs of those involved.

7.4 Risks should be identified whether or not their sources are under KCC's direct control, as they have the potential to impact on achievement of objectives, causing great damage or creating significant opportunity.

Risk Analysis

7.5 The aim of risk analysis is to build understanding of the nature of risk and its characteristics including, wherever possible, the level of risk. It involves consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness. Analysis techniques can be qualitative, quantitative or a combination of these, depending on the circumstances and intended use.

7.6 Risk Analysis considers factors such as:

- the likelihood of events and consequences occurring
- the type and scale of consequences
- complexity, connectivity and volatility
- time-related factors
- the effectiveness of existing controls
- sensitivity and confidence levels

7.7 KCC uses a common set of risk criteria to foster consistent interpretation and application in defining the level of risk, based on the assessment of the likelihood of the risk occurring and the consequences should the event happen. Below is KCC's 5x5 Risk Matrix used to determine risk ratings (outlined below), where the likelihood score is multiplied by the impact score in order to achieve an overall rating of between 1 and 25:

Likelihood	Very likely	5	5 Low	10 Medium	15 Medium	20 High	25 High
	Likely	4	4 Low	8 Medium	12 Medium	16 High	20 High
	Possible	3	3 Low	6 Low	9 Medium	12 Medium	15 Medium
	Unlikely	2	2 Low	4 Low	6 Low	8 Medium	10 Medium
	Very Unlikely	1	1 Low	2 Low	3 Low	4 Low	5 Low
RISK RATING MATRIX			1	2	3	4	5
			Minor	Moderate	Significant	Serious	Major
			Impact				

7.8 Providing sufficient information is known, during assessment each risk is to be assigned a ‘current’ and ‘target’ risk rating. The ‘current’ risk rating refers to the current level of risk, taking into account any mitigating controls already in place and their effectiveness. The ‘target’ rating represents what is deemed to be a realistic level of risk to be achieved once any additional actions have been put in place. Depending on our risk appetite and the level of direct control we have over the risk, the aim may be to contain the risk at the current level.

7.9 For risks that are judged to have reached their ‘target’ residual level, the Risk Owner and appropriate management team may wish to manage the risk at a lower level, unless management wishes to continue to monitor effectiveness of controls as part of the regular and structured risk management process. Alternatively, the risk can be withdrawn if it is no longer judged as relevant or significant.

7.10 Risk assessments and heat maps used for more conventional risks should be complemented by structured, creative discussions across services that bring different and collaborative risk perspectives on a topic. This will help us to better identify emerging risks and understand potential risk trajectories as well as ‘knock-on’ effects.

Risk Evaluation

7.11 Once analysed, risks will be evaluated to compare the results against the nature and extent of risks that the organisation is willing to take or accept to determine where and what additional action is required.

Risk Appetite, Tolerance and Escalation

7.12 Kent County Council recognises that risk is inherent in delivering and commissioning services and does not seek to avoid all risk, but instead aims to have an ‘open’ approach to risk, appropriately balancing risk against reward, with risks managed in a proportionate manner.

7.13 This will require an approach that allows flexibility and support for well-informed and considered risk taking, promoting transparency and effective risk management, while maintaining accountability. While risks defined as ‘high’ are to be managed down to a tolerable level wherever possible, it is important that risks across the Authority are not over-controlled.

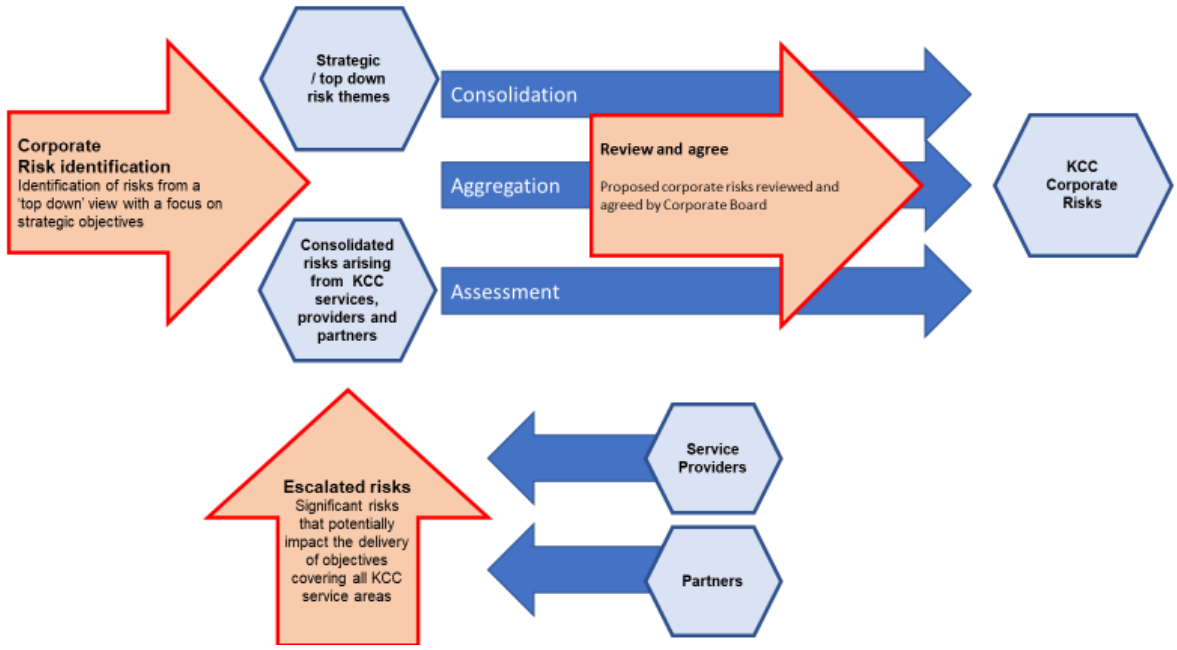
7.14 It is not realistic for the County Council, with its diverse range of services and duties, to have just one definitive application of risk appetite across the entire organisation. Instead, risk appetite should be set with reference to the

strategy for service delivery in each particular area. However, examples of risks that would be seen as intolerable are those that are likely to:

- Negatively affect the safety of our service users, residents or employees.
- Severely damage the Authority's reputation.
- Lead to breaches of laws and regulations.
- Endanger the future operations of the County Council (i.e. by exceeding the risk capacity of the organisation – the amount of risk that the Authority can bear).

7.15 In addition, to aid managers in understanding what risks are acceptable, our appetite for risk is implicitly defined within our standard for determining risk levels (see section 7.7 above). Risks rated as "High" will be deemed to have exceeded tolerance levels and will be subject to escalation to the next management level for review and action. The target rating for a risk is expected to be 'medium' or lower. In the event that this is not deemed realistic in the short to medium term, this shall be discussed as part of the escalation process, and this position regularly reviewed with the ultimate aim of bringing the level of risk to a tolerable level.

Risk Escalation, Consolidation and Aggregation



7.16 Depending on the nature of the risk and availability of objective risk measures, tolerances will be agreed for Key Risk Indicators. Breaching those tolerances will mean increasing or decreasing the risk rating accordingly.

Risk Treatment

7.17 Potential benefits derived in relation to the achievement of objectives are to be balanced against the costs, efforts or disadvantages of implementation.

7.18 Justification for the design of risk treatments and the operation of internal control is broader than solely financial considerations and should consider all of the organisation's obligations, commitments and stakeholder views.

Risk Monitoring

7.19 The frequency of risk assessment, analysis and review should be a function of how fast risks are emerging and the level of their materiality rather than determined by traditional institutional administrative cycles.

7.20 However, as a minimum, risks should be reviewed every 3 months, with risks rated as 'High' subject to more detailed and frequent monitoring. It is expected that in addition to the timely reviewing of individual risks by risk owners, key risks are subject to structured collective discussion by management teams, focusing on changes to the existing risk profile, trends and any emerging risks.

7.21 The Corporate Risk Manager may initiate a review of a corporate risk if it is felt that either external or internal changes are likely to impact on the level of risk exposure for the council.

7.22 Ongoing monitoring should support understanding of whether and how the risk profile is changing and the extent to which internal controls are operating as intended to provide reasonable assurance over the management of risks to an acceptable level in the achievement of organisational objectives.

Risk Reporting

7.23 Senior Officers and elected Members must receive unbiased information about the organisation's principal risks and how management is responding to those risks.

7.24 Reporting will take into account differing stakeholders and their specific information needs and requirements; cost, frequency and timeliness of reporting; method of reporting; and relevance of information to organisational objectives and decision-making.

7.25 As a public service body, it is imperative that we demonstrate transparency and accountability for managing the risks that impact on our staff, service users and residents. Therefore, our corporate risks shall be reported regularly in public forums.

7.26 The Corporate Risk Register is to be presented to Cabinet annually after its more formal annual refresh, in addition to any occasion where there has been a significant change to the Council's overall risk profile.

7.27 The Corporate Risk Register is also to be reported to the Governance & Audit Committee six-monthly for assurance purposes, alongside a summary of directorate risks.

7.28 Corporate Risks are subject to "deep dive" reviews by Corporate Board and the Governance & Audit Committee, with those responsible for the management of risks present, at an appropriate frequency, depending on the nature of the risk.

7.29 Progress against objectives set out in this Policy and Strategy will be reported to the Governance & Audit Committee annually.

8. Cultural Factors

8.1 Human behaviour and culture significantly influence all aspects of risk management at each level and stage. Several vital elements of an effective culture for risk are embedded within our organisational values and cultural attributes that we strive for as an organisation. In particular:

- KCC Values
  - We are brave. We do the right thing, we accept and offer challenge
  - We are curious to innovate and improve
  - We are strong together by sharing knowledge

- KCC Cultural Attributes
  - Flexible/agile – willing to take (calculated) risks
  - Empowering – our people take accountability for their decisions and actions
  - Curious – constantly learning and evolving

9. Review of this Policy

9.1 It is the responsibility of the Governance and Audit Committee to: *'On behalf of the Council ensure that risk management and internal control systems are in place that are adequate for purpose and are effectively and efficiently operated.'* Internal Audit will support their role in assuring its effectiveness and adequacy.

9.2 Information from Internal Audit and from other sources will be used to inform recommended changes to the policy and framework at least annually. Any

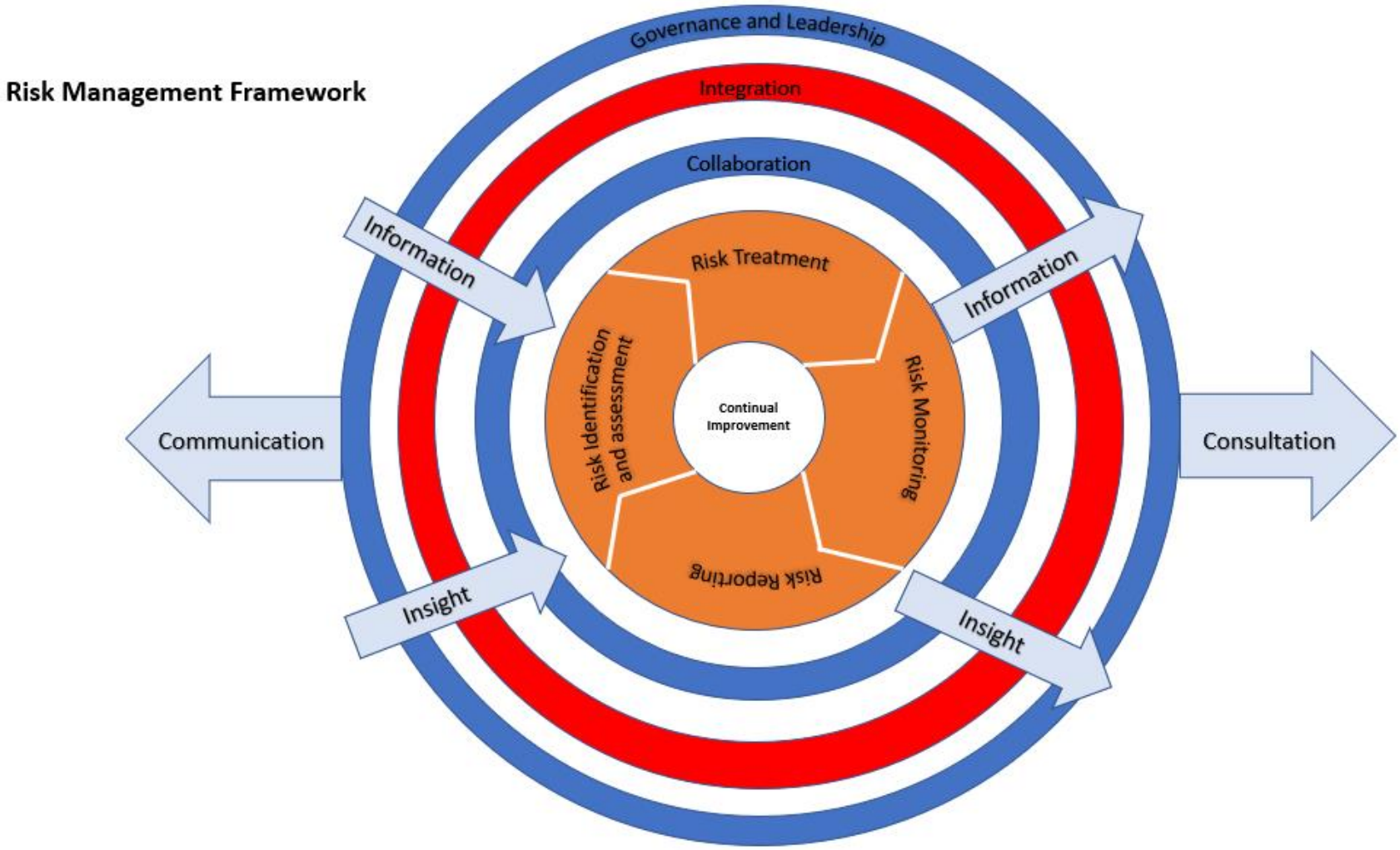
changes will be presented to the Governance and Audit Committee for approval before publication.

10. Roles and Responsibilities

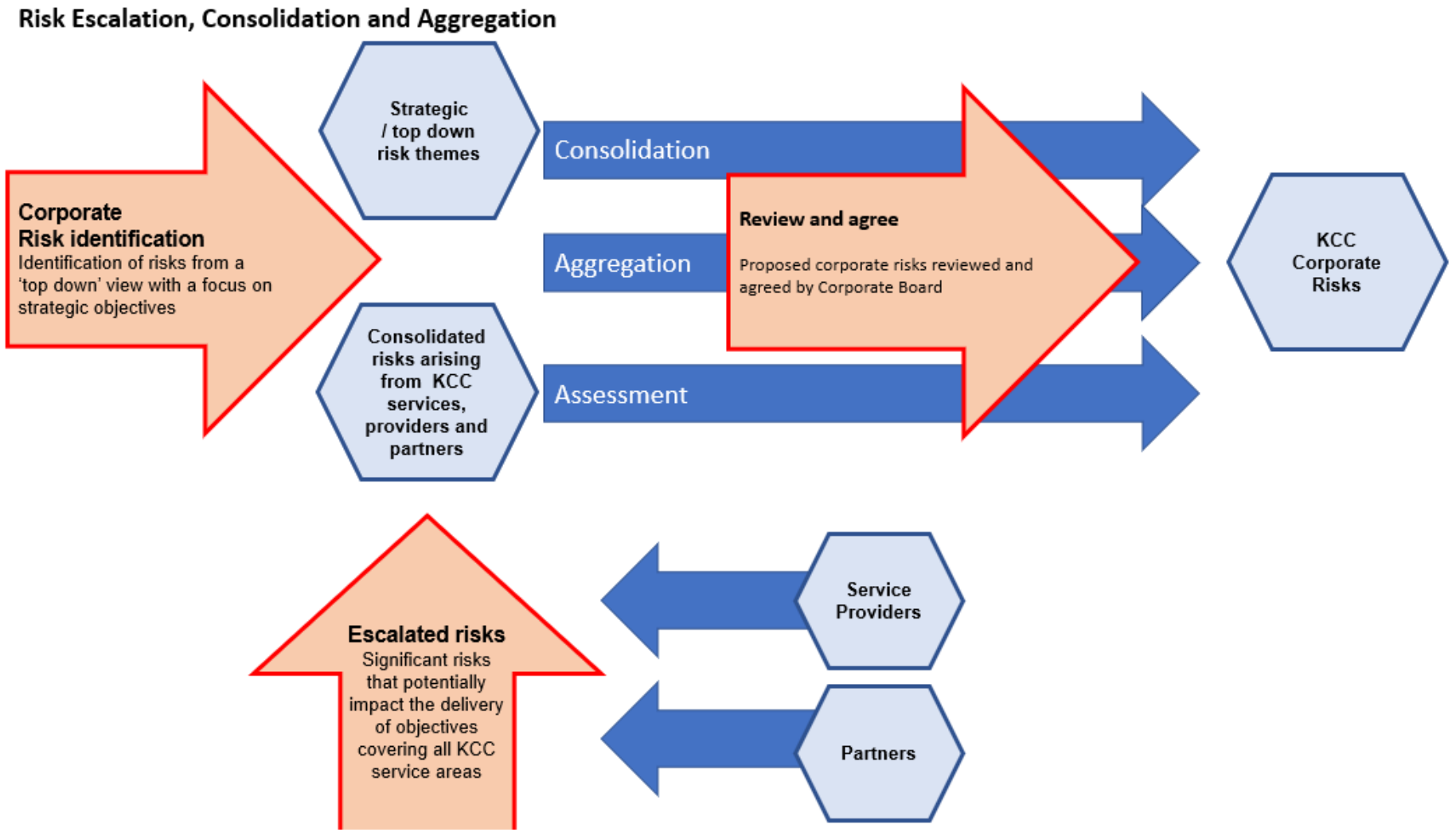
Group or Individual	Responsibilities
Elected Members of the County Council	Seek to explore, understand and scrutinise risks in the process of formulating policy and decision making.
Governance & Audit Committee	On behalf of the County Council, ensure that risk management and internal control systems are in place that are adequate for purpose and are effectively and efficiently operated. Includes approval of KCC's Risk Management Policy & Strategy.
Cabinet	Responsibility for the operation of the risk management framework, including the establishment of the Council's risk appetite.
Cabinet Members	Responsibility for the effective management of risk within respective portfolio areas and ensuring that risks are considered in all decisions they make.
Cabinet Portfolio Holder for Corporate Risk	Ensure effective risk management arrangements are put in place.
Cabinet Committees	To provide pre-decision scrutiny to ensure that due consideration is given to associated risks.
Corporate Director Finance (Section 151 Officer)	Active involvement in all material business decisions to ensure immediate and longer-term implications, opportunities and risks are fully considered.
Head of Paid Service	Responsibility for the overall monitoring of strategic risks across the council, including the endorsement of priorities and management action. Responsible for ensuring sufficiency of risk management resources.
Corporate Management Team (CMT)	Adopt the Risk Management Policy and Strategy, ensuring the Council manages risks effectively. Actively consider, own and manage key strategic risks affecting the Council through the Corporate Risk Register. Promote and demonstrate the behaviours and values that support well-informed and considered risk decision-making. Promote the integration of risk management principles into the

	culture of the Council and its partners.
Directorate Management Teams (DMTs)	Responsibility for the effective management of risk within the directorate, including risk escalation and reporting to the Corporate Management Team as appropriate.
Divisional Management Teams (DivMTs)	Responsibility for the effective management of risk within the division, including risk escalation and reporting to the Directorate Management Team as appropriate.
Corporate Risk Manager	Promote a positive risk management culture within KCC, developing and implementing the risk management framework and strategic approach and continuing to develop and embed an effective infrastructure for managing and reporting risk. Facilitate maintenance of an up to date Corporate Risk Register and provide reports on corporate risk to Governance & Audit Committee, Cabinet Members and the Corporate Management Team. Facilitate the risk management process within the Council and advise on developments on risk management. Assist key individuals with implementing and embedding risk within key Council areas and provide guidance, training and support as required.
Corporate Risk Team	Act as corporate advisors of risk at a strategic level. Day-to-day responsibility for developing and co-ordinating risk management across the Council, providing advice, support and training and contributing to the ongoing reporting and analysis of risks. Develop oversight, transparency and coordination of major change activity across the Council, including reinforcing KCC's risk management framework throughout major change activity. Continually improve and update corporate risk management procedures based on current best practice and lessons learned.
Internal Audit	Assess the effectiveness of the risk management framework and the control environment in mitigating risk.
Directors and Managers	Ensure that effective risk management arrangements are in place in their areas of responsibility to ensure the Council's exposure is at an acceptable level. Promote and demonstrate the behaviours and values that support well-informed and considered risk taking, while maintaining accountability. Encourage open and frank conversations about risks, ensuring appropriate reporting and escalation as required.

All elected Members and Staff Members	Identify risks and contribute to their management as appropriate. Report inefficient, unnecessary or unworkable controls. Report loss events or near-miss incidents to management.
In relation to individual risks:	
Risk Owner	Named individual or role who is accountable for the management and control of all aspects of the risks assigned to them, including determining, authorising, implementing and monitoring the selected controls and actions to address the threats and maximise the opportunities.
Control Owner	The individual or group accountable for ensuring or providing assurance that the specified management control is effective and fit for purpose.
Action Owner	A nominated owner of an action to address a risk. Required to manage action on the risk owner's behalf and to keep them apprised of the situation.



Larger version of diagram from section 6.3



Larger version of diagram from section 7.15