Kirklees Council Risk Management Framework:

Risk Management Strategy & Guidance

July 2024

Contents

1. Aims & Objectives

The Risk Management Framework at Kirklees Council is set out in three linked documents. The Risk Management Policy explains the Kirklees Council approach to risk management, the aims and objectives of the Policy (what we are seeking to achieve) and the roles and responsibilities of those involved. Alongside, the Risk Management Strategy & Guidance provides further detail on the framework that risk management follows, support and guidance for those involved in managing and reporting on risk, and detail on how the objectives of the Policy are to be achieved. Additionally risk register and corporate risk report

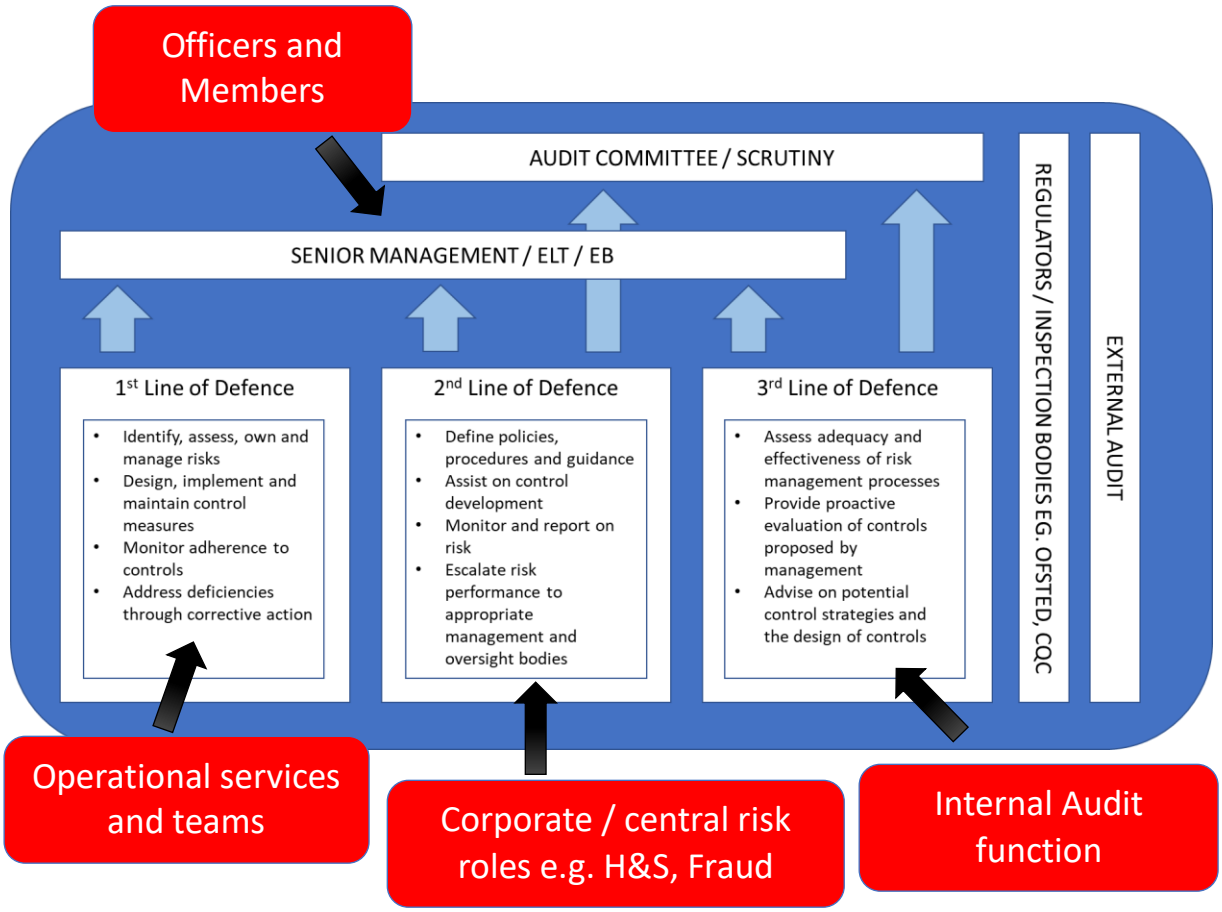
2. Risk Appetite

Risk appetite describes the amount and type of risk that an organisation is willing to take in order to meet its strategic objectives. The intention is to operate within the agreed risk appetite, where activity is considered to be outside of risk appetite appropriate action must be taken to resolve.

Definitions of risk appetite levels for key strategic risk categories are set out within the Risk Appetite Statement

3. The Three Lines of Defence

The council follow the “three lines of defence” model which supports the assertion that everyone across the council has some responsibility for risk management. The lines of defence have a common objective: to help the organisation achieve its objectives through effective management of risks.



4. Risk Management Process

Our risk management processes are 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 that support achievement if intended outcomes and manage risks to an acceptable level
- The design and operation of integrated, insightful and informative risk monitoring
- Timely, accurate and useful risk reporting to enhance the quality of decision making and to support officers and members in meeting their responsibilities

4a. Risk Identification

This is the process of determining risks that could potentially prevent the Council achieving its objectives. This could be at a strategic or service level. Directorate and Service leads must have a strong understanding of the threats (and opportunities) associated with the delivery of agreed strategies and plans. Additionally, an understanding of the relevant statutory duties is required, and a robust framework to demonstrate compliance with these requirements.

Useful inputs to consider:

- Complaints data, including published Ombudsman findings
- Professional networking insight – is there read across to Kirklees?
- Insurance claims / payouts
- Feedback from regulatory oversight bodies (eg. Ofsted, CQC, RSH)
- Published guidance / best practice
- Recommendations identified through Internal Audit activity
- Findings included within External Audit reports

Sources of risk will vary depending on each Service area however the following provides a generic list of risk sources to consider initially:

- Staff – training, experience, tenure, motivation, retention
- Stability of service offering – new service, new customers, changed delivery methods
- Manual processes / Automation – oversight of both
- IT infrastructure / applications
- Supplier selection and ongoing contract management
- Partnership relationships and governance
- Recent / upcoming regulatory change
- Changes to what is seen as good practice.
- New products and technologies that impact on the way activity is delivered
- Customer expectations
- Information assets
- Vulnerability of service users
- Statutory obligations

Further guidance and assistance is available from the Corporate Risk Team if required.

All risks that could impact on the successful delivery of Service objectives should be documented, even if the risk is deemed to be effectively controlled.

Emerging Risks should also be recorded within Directorate Risk Registers. Emerging Risks are defined as “a future internal or external event or trend, which could have a material adverse impact on the council, our communities or our staff but where the probability, timescale and / or materiality are difficult to accurately assess”.

Any emerging risk that is serious should be drawn directly to the attention of the corporate risk team as it appears to be emerging (irrespective of the timing of the general reporting)

An Issue is something that is already happening, while a risk is something that has the potential of happening in the future. If something is certain or has already happened / is happening, then that is an Issue. Issues should be recorded on an Issues log. Actions that are required to address the issue should be identified and tracked to completion.

4b. Risk descriptions

Good quality risk descriptions should be clear, concise, meaningful and well defined. Identifying the main causes of risk and articulating them in the risk description enables the Council to better understand the controls required to manage and mitigate the risk.

Cause / Risk / Effect

It is essential to write clear risk statements in order to understand them, assess their importance, and communicate them to key stakeholders across the organisation. The key point is that if people understand what the risk is they can then help to mitigate it.

- What the risk is (event)
- What the trigger is for the risk ie what will cause it to happen (cause)
- What the impact of the risk is if it happens (consequence)

The more precisely and concretely you formulate your risks, the more accurately you can identify measures to monitor the risk, and mitigants to reduce the likelihood / impact of the risk. Only if you formulate the risks systematically and carefully can you ensure that:

- everyone understands exactly what kind of risk it is.
- the identified risk is accepted as relevant
- the right measures are taken

A description at too high level, such as “something unexpected could happen during the project”, is of course not useful, as no meaningful measures are possible at this high level. However, too much detail can result in the risk being description being too narrow.

The recommended format for risk descriptions is as follows:

The risk of “A”, caused by “B”, leading to “C”

Failure of “X”, caused by “Y”, leading to “Z”

What risks are not:

- A statement of fact
- A list of tasks / activities that need to be completed
- Extracts from a job description / role profile
- An under or unfunded budget pressure (though the consequences of this might be a risk)
- An issue (a risk that has already crystalised)
- Overly generic

Map risk to risk type.
All risks must be mapped to a primary risk type. It is likely that risks will impact more than one risk type, and in this instance additional risk types can be also listed.

Principal Risks:

- Operational / Service Delivery
- Legal, Regulatory & Compliance
- Physical Assets
- Financial
- Third Party
- People & Culture
- Environmental
- Safeguarding
- Transformation & Change
- Reputation
- Data, information management or cyber

4c. Risk Assessment

Risks are assessed and scored using the Council's approved Risk Assessment Matrix. The risk assessment matrix provides a tool to ensure that the Council can consistently assess the potential impact and likelihood of a risk occurring.
This assesses the probability or likelihood of a risk occurring on a scale of 1-5 and the Impact, were a risk to crystallise.

The score should be based on the **most likely scenario** to occur. The risk register should not reflect worst case scenario modelling.

Inherent Risk Assessment

The inherent (or gross) risk is scored assuming legal and statutory requirements are adhered to but without taking into consideration any additional mitigants and / or controls that are operating.

Residual Risk Assessment

Residual (or net) risk is the level of risk that is left once all mitigants and controls are in place and operating effectively. It is an assessment of the likelihood of a risk crystallising and what the impact might be, taking into account the key controls already in place and other external factors.

Target Risk Assessment

The target risk assessment indicates the position that the risk could move to on the risk assessment matrix assuming:

- the effective operation of all existing controls
- completion of all additional actions that have been identified

- there are no unanticipated changes in the internal or external operating environment (ceteris paribus)

A timeline of 36 months is used to inform the target risk assessment. This field is recommended, however becomes mandatory for all risks that appear on the corporate risk register.

Likelihood measures

Probability	Rare	Unlikely	Possible	Probable	Almost Certain
Score	**1**	**2**	**3**	**4**	**5**
Frequency *When do you expect it to happen?*	This will probably never happen	Not expected to happen over a 3 year horizon	Might happen within 3 years	Is likely to happen within 3 years	Is expected to happen within the next year
Likelihood *Chance of it happening over a 3 year time period*	Less than 5% (0-5%)	Around 10% (5-15%)	Around 25% (15-40%)	Around 60% chance (40-80%)	Around 90% chance of this happening (80-100%)

Impact measures

Impact	Insignificant	Minor	Moderate	Major	Very Significant
Score	**1**	**2**	**3**	**4**	**5**
Finance	Zero or negligeable financial impact	<£100k	>£100k <£1m	>£1m <£5m	>£5m
Legal, Compliance, Regulation	No or minimal impact or breach of guidance / statutory duty. Minor civil litigation risk	Minor breach of statutory legislation / regulation. Reduced performance rating if left unresolved.	Single breach in statutory duty. Challenging external recommendations. Major civil litigation and / or local public inquiry.	Several breaches in statutory duty. Enforcement action and improvement notices. Major civil litigation and / or national public inquiry. Critical report.	Government intervention or criminal charges. Multiple breaches in statutory duty. Prosecution. Severely critical report.
Public Health (inc Health & Safety)	Environmental incident with no lasting detrimental effect. No impact.	Medical treatment required, potential long term injury or sickness.	Fails to prevent extensive, permanent injuries or long term sickness Medium term	Fails to prevent death, causes extensive permanent injuries or long term	Responsible for death of employee / resident. Permanent, major environmental

		Short term public health or environmental incident (weeks).	major public health or environmental incident (up to 1 year).	sickness Long term major public health or environmental incident	or public health damage.
Reputation	No media awareness	Short lived local media attention	Prolonged local media attention	Adverse national media attention	Prolonged negative national media attention
Service Delivery	Limited or no impact	Slight delay to peripheral objectives	Delay to achievement of council objectives	Significant threat to council objectives	Core objectives cannot be delivered

4d. Risk mitigation

Controls must be identified and documented for all risks.

Preventative Controls: these are controls that are designed to prevent errors or irregularities from occurring and risks materialising in the first place.

- Segregation of duties
- Employee background checks
- Use of safes for storage of cash / sensitive documents
- Encryption of sensitive data
- Defined access rights to IT systems
- Professional qualifications
- Training
- Documented policy and procedures
- Inspection & maintenance schedules
- Peer review

Detective Controls: these are designed to find errors or irregularities after they have occurred. By their nature they tend to be resource intensive and are therefore more expensive to implement

- Security alarms
- Bank reconciliations
- Stock takes and inventory counts
- Cost Centre management (eg. review of Purchase Card spend)
- Incident reporting process
- Case reviews / Quality Assurance

Limiting or Corrective Controls: these controls are designed to limit the impact and extent of damage were the risk to crystallise

- Backup and recovery of data
- Insurance cover
- Business continuity / Incident management plans

All risk mitigation should be proportionate to the level of risk that we are facing as an organisation. Every control has an associated cost, and it is important that the control represents an effective use of council resources.

The effective use of controls will constrain a risk to an acceptable level, rather than eliminate it all together.

Controls must be measurable, and their performance reported on. It is not acceptable to make generic statements, reference to who operates the control, the frequency and reporting mechanisms should be included.

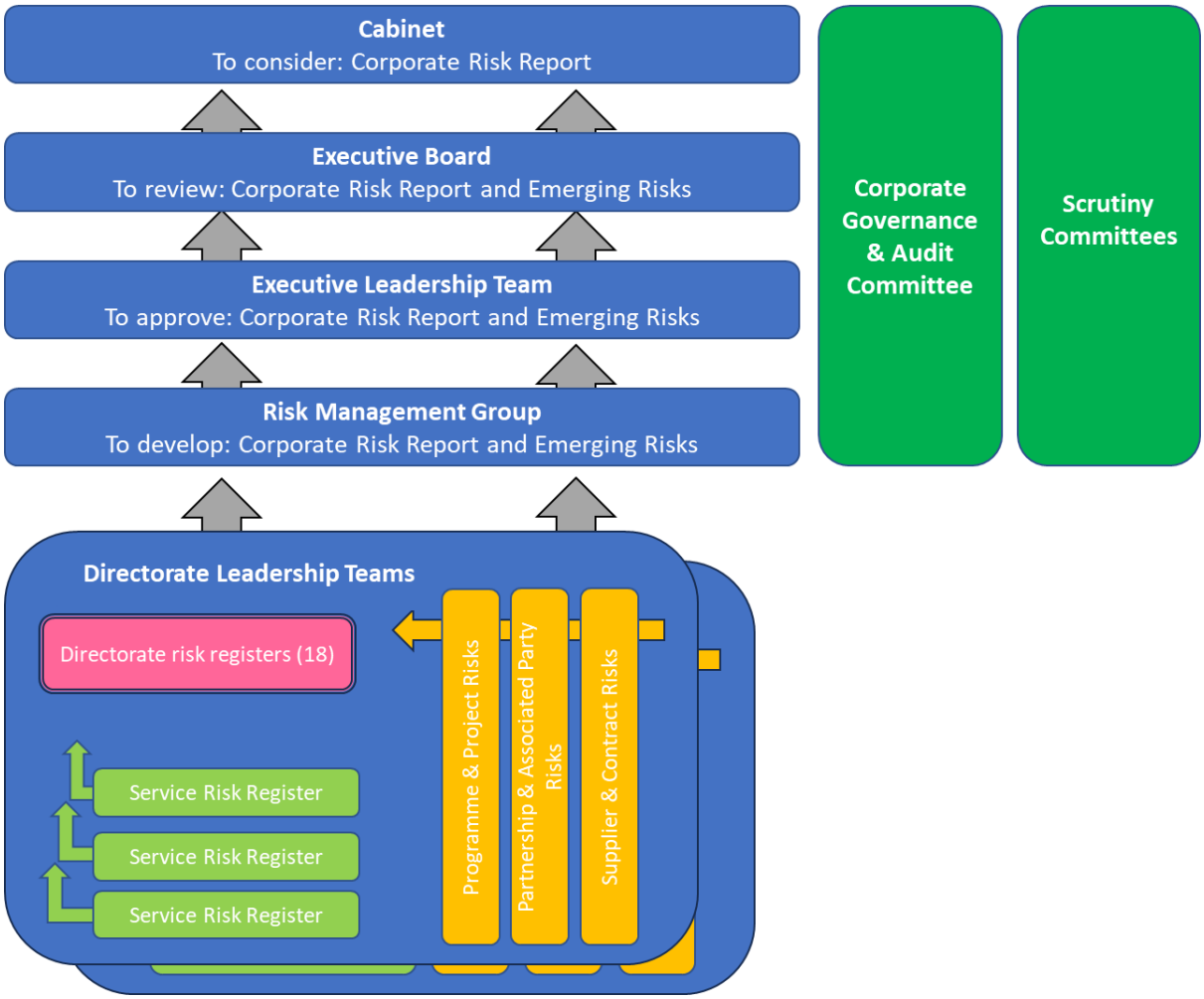
Unacceptable control description:

- Staff training

Acceptable control description:

- Individual training needs are assessed and recorded by line managers at induction for new starters and when staff change roles as a result of promotion / secondment
- Role specific training requirements are documented in the Service Training Guide
- Training completion rates are monitored through the quarterly directorate people forum

4e. Monitoring and reporting



All Directorates must maintain a Directorate level risk register. Service Directors may choose to implement risk registers at a lower level within their Directorate (eg. at Service level). Factors that may influence this decision include the size of the Service, type and breadth of activities undertaken, experience of the leadership team in managing risk and the extent to which risk management activities are already embedded within operational processes.

The Council has a single, standard risk register template that is used to record and monitor risks organisation wide. Directorate risk registers must use the approved template.

Directorate Risk Registers must be reviewed by the relevant Directorate Management Team on a frequent basis, and at least every three months to ensure that risks are being effectively managed, that they remain accurate and reflect current risk exposure and control performance.

The risk management process is managed on a day-to-day basis at Head of Service and Service Manager level.

Each identified risk must have a Risk Owner. It is their responsibility to manage the risk, and report as appropriate about any deterioration or improvement in the position. Ownership of high-level corporate risks are held by Strategic Directors and Statutory Officers, whilst at directorate and service level they can be held by the Director, a Head of Service, a Service Manager, or another relevant role holder (eg. Project Manager). Regardless of role, the Risk Owner must have the ability to make decisions and hold authority and resource to command actions that are appropriate to control or mitigation of the risk. The Risk Owner may not necessarily operate all of the controls that are aligned to the risk, but they require oversight of control performance.

It is the responsibility of the Risk Owner to ensure that the risk record remains accurate. To achieve this the Risk Owner should have consideration of the following:

- Am I aware of any internal or external developments that have altered the inherent probability and impact rating?
- Do the documented controls accurately reflect the processes in place to mitigate this risk?
- Are there performance indicators to support control performance?
- Do additional risk mitigation actions need to be put in place to further control the risk?
- Have any assurances been received on the effectiveness of the control management framework (self-assessments, Internal Audit, External quality reviews eg. OFSTED, CQC)

The management of project level risks is undertaken outside of the corporate risk framework using standard templates to ensure a consistent approach. Link here. It is expected that projects that are reporting as 'red', indicating significant issues relating to time / quality / budget, will also appear on Directorate Risk Registers, due to the potential impact on existing Directorate level risks.

The Risk Management Group meets on a quarterly basis to:

- Review the Corporate Risk Register and consider if this represents an accurate reflection of corporate strategic risks facing the Council, prior to this being reported to Executive Team.
- Review the Emerging Risks register and highlight any new sources of potential risk for inclusion.
- Where appropriate, escalate Directorate / Service Operational risks to the Executive Team to consider inclusion on the Corporate Risk Register.
- Investigate other areas of potential risk and make mitigation recommendations.

Terms of Reference for this meeting can be found here.

Corporate Risk Reporting

The Corporate Risk Register will be reviewed by the Executive Leadership Team (ELT) and Executive Board (EB) on a quarterly basis. ELT and EB will be informed of the risk exposure across the organisation, including detail of key strategic and

business critical risks, the risk profile outlook, and the activity underway to manage and mitigate identified risks.

The Corporate Risk Register will be reported to the Corporate Governance & Audit Committee on a biannual basis. Further detail on risks that are presenting a specific concern may be requested by members, and in this instance the risk owner will be required to attend to provide further detail.

The Risk Management process will be subject to standard assurance activity including Internal Audit review and external audit oversight. The Annual Governance Statement (AGS) will include assurances around risk management and other governance arrangements.

5. Embedding Risk Management across the Council

For risk management to be an effective and meaningful management tool it must be an integral part of key management processes and day to day working. Risk, and risk management needs to feature in core business processes including, but not limited to:

Corporate decision making
Significant risks, which are associated with a policy or actions to be taken, must be included in appropriate reports. Corporate templates require risk commentary to be included as part of the submission. Advice should be sought from the Corporate Risk Team where associated risk impacts are unclear.
Intranet | Decision making and report writing (kirklees.gov.uk)

Finance / budget planning
Decision to balance outcomes, outputs and planned expenditure must recognise risks associated. Corporate templates require risk commentary to be included as part of the submission

Strategy & Policy development:
The content and trajectory of key service, directorate and corporate risks are used to inform the development of Our Council Plan and ensure strategy and policy decisions are made with full understanding of the potential impact on the risk profile of the organisation.

Programme and Project risks:
Risks to Project / Programme delivery must be managed following established project management templates. The approved RAIDD log can found here Intranet | Project and change management (kirklees.gov.uk).

Review of, and if appropriate escalation, of risks should take place through existing project reporting routes, as agreed with the project sponsor.

It is expected that risks to delivery of strategically important projects will be included within the Directorate Risk Register to ensure adequate visibility. The Project Board should recommend that the risk is included within the relevant Directorate level Risk Register.

Supplier / contractor risks:
Robust contract management procedures should include the recording and regular review of associated risks and identified mitigants. These requirements are set out in the Contract Procedure Rules. Intranet | Stage 6 - Contract management (kirklees.gov.uk)

Where material, it may be appropriate to record specific risks relating to suppliers and / or contractors on Directorate level Risk Registers. Examples could include:

- Possible reputational damage to the council through association with a specific third party
- Concerns about the ongoing financial viability of a specific third party

- Poor performance by a third party that is impacting on service delivery.

Partnership / Associated Parties risks:
Risks that arise from working with partners, or with associated parties (whether within a contractual framework or not) must be identified, recorded, managed and escalated as appropriate. The relevant Service Director is responsible for determining the approach to be taken for each specific third party.

Where material, it may be appropriate to record specific risks relating to partners and / or associated parties on Directorate level Risk Registers. Examples could include:

- Possible reputational damage to the council through association with a specific third party
- Concerns about the ongoing financial viability of a specific third party
- Poor performance by a third party that is impacting on service delivery.

Information Governance:
Data Protection Impact Assessments (DPIAs) are conducted on all work involving the use of personal information to assess the level of information risk and provide assurance that information is being processed fairly and lawfully. Intranet | Information governance (kirklees.gov.uk)

Insurance:
The Council's insurance strategy is managed by the Insurance Team, details of uninsured and uninsurable risks are available on request.

Health & Safety:
The Council has a specific risk assessment policy to be followed in relation to Health & Safety Risk. Corporate-Safety-Index-of-Health-and-Safety-Documents (kirklees.gov.uk)

Emergency Planning and Business Continuity:
Corporate Risk Management works collaboratively with the Emergency Planning and Business Continuity teams, reviewing resilience reports on a regular basis for potential new or worsening risks. West Yorkshire Prepared is the Local Resilience Forum for West Yorkshire, producing and maintaining the Community Risk Register for the region.

6. Document governance

6a. Linked documents:

Risk Appetite Statement

Risk Management Policy

Risk Assessment Matrix

Risk Register Template

6b. Sources:

HMG
The Orange Book
Risk Appetite Guidance Note

ALARM
Risk Management Toolkit
Risk Reporting Guide

6c. Key contacts:

Corporate Risk Management
Martin Dearnley
Alice Carruthers

Project Management
Clair Ashurst Bagshaw
TransformationPMO@kirklees.gov.uk
Rashid Mahmood
PMO.mailbox@kirklees.gov.uk

Procurement
Jane Lockwood
Procurement@kirklees.gov.uk

Insurance
Karen Turner
Insurance.Section@kirklees.gov.uk

Health & Safety
Sean Westerby
Khalid Razzaq

Business Continuity & Resilience

Martin Jordan

Information Governance
Erin Wood
Information.Governance@kirklees.gov.uk

Partnerships
Stephen Bonnell
Jonanthan Nunn

6d. Document history

Document owner: **Head of Internal Audit & Risk**

Approval body: **Cabinet**

Review period: **Annual review**

Document history:

Version	Comments	Date
0.1	First draft	June 2023
0.2	Incorporating feedback from Head of Risk and Monitoring Officer	Dec 2024
0.3	Incorporating feedback from Strategic Director and SLT review Removal of detail relating to risk appetite	March 2024
0.4	Feedback received from ELT	April 2024
	Corporate Governance and Audit Committee	June 2024
	Cabinet	July 2024

Appendix 1: Completing the Risk Register

The risk register is the tool which facilitates data collection and records all identified risks, their mitigations and associated scoring of impact and likelihood. A standard template for data collection has been designed and includes the following categories:

Risk Reference: A unique sequential number for each risk. The risk reference is prefixed by a 2/3 letter abbreviation indicating the Directorate. Eg. CAS for Communities and Access Services.
Risk References should not be re-used.

Risk Short Name: Brief summary of the risk.

Date raised: Date that risk was added to the risk register.

Risk Description: The risk description section is split into 3 sections to aid clarity in determining the actual risk, as opposed to a cause or consequence of a risk.
Risk – "The risk of…" what happening?
Cause – what will cause the risk to happen eg. failure to follow procedures / guidance, insufficient resource, dispute with third party, backlog of maintenance, increase in demand, inadequate training,
Consequence – for example this could be loss of income, increase in cost, breach of statutory obligations, regulatory censure, reputational damage.

Risk Owner: It is recommended that this is documented as a role / job title with the incumbent's name following. Eg. 'Corporate Customer Standards Manager – Chris Read'

Primary risk category: Singular risk category to be selected from the drop-down box.

Secondary Risk category: Additional risk categories can be selected from the drop-down box.

Inherent Risk score: Risk to be scored using the corporate risk assessment matrix assuming no controls are in place. How frequently would this risk occur without controls? What would the severity be?

Residual Risk score: Risk to be scored using the corporate risk assessment matrix assuming controls, as detailed, are operating effectively.

Target Risk score: An indication of the level of risk that would be within risk tolerance and could be achieved within a medium term (3 year) timeframe.

	This score should be determined in conjunction with the Risk Appetite Statements. This is a mandatory field for risks that are escalated to the Corporate Risk Register. It is an optional field for all other risks.
Controls:	Defined as 'processes that are in place to mitigate a risk through reducing probability of a risk occurring, or the impact were the risk to occur'. Risk Owners should have processes in place to monitor whether controls are operating as expected and take appropriate action if they are found to be ineffective. All controls should have an owner. This is not necessarily the risk owner. It is expected that control performance will be assessed as part of internal audit reviews, where relevant.
Actions:	Additional activity that is required to bring the risk within risk appetite. Actions require action owners and timelines. Risk Owners should have processes in place to monitor progress of actions and escalate where insufficient progress is being made. Not all risks will have additional actions.
Quarterly update:	Provide supporting comments to explain any change, or not, to likelihood, impact, or both. This is expected to reflect the impact of changes in status of action(s) or control(s), or the impact of any newly established controls. Internal/external influences may also affect the risk score.
Outlook:	Simple assessment of the risk trajectory - improving, deteriorating or remaining the same?