Public Document Pack

Democratic Services

To: All Members of the Strategy and Resources Committee

Dear Councillor,

STRATEGY AND RESOURCES COMMITTEE - TUESDAY, 14TH NOVEMBER, 2023 , Council Chamber - Epsom Town Hall

Please find attached the following document(s) for the meeting of the Strategy and Resources Committee to be held on Tuesday, 14th November, 2023.

4. **RISK MANAGEMENT STRATEGY REVIEW** (Pages 3 - 30)

The annual review of the Risk Management Strategy has been conducted by officers. This version incorporates recommendations from our internal auditors (SIAP), and addresses points raised by council members and officers over the last year.

For further information, please contact democraticservices@epsom-ewell.gov.uk or tel: 01372 732000

Yours sincerely

Chief Executive

This page is intentionally left blank

RISK MANAGEMENT STRATEGY REVIEW

Head of Service:	Andrew Bircher, Interim Director of Corporate Services
Wards affected:	(All Wards);
Urgent Decision?(yes/no)	No
If yes, reason urgent decision required:	N/A
Appendices (attached):	Appendix 1 – Updated Risk Management Strategy

Summary

The annual review of the Risk Management Strategy has been conducted by officers. Attached at Appendix 1 is an updated Strategy. This version incorporates recommendations from our internal auditors (SIAP), and addresses points raised by council members and officers over the last year.

Recommendation (s)

The Committee is asked to:

(1) Approve the revisions to the Risk Management Strategy as attached at Appendix 1.

(2) Agree to run a workshop with key councillors and officers to review: a) the council's risk appetite, and b) risk targets, and how these could be applied in practice.

1 Reason for Recommendation

1.1 The Risk Management Strategy ("Strategy") is reviewed annually by officers, and non-administrative updates are brought to this committee for approval, in line with its terms of reference.

1.2 Revisions have been made and an updated Strategy is attached at Appendix 1. The revisions seek to address the recommendations raised by our internal auditors, the Southern Internal Audit Partnership (SIAP), and points raised by councillors and officers over the last year.

1.3 In addition, officers believe further consideration of a) how the council manages its risk appetite, and b) using risk targets, could strengthen risk management practice across the organisation. Therefore, the Committee is asked whether it would like officers to pursue these points, in consultation with key councillors, or whether it is content with current practice.

2 Background

2.1 An audit of risk management in 2021-2022 coincided with the expiry of the council's Strategy.[1] Consequently, a new Strategy was drafted in 2022,[2] and approved by this Committee in July of that year. Following this, the Audit and Scrutiny Committee commissioned a review of the newly approved Strategy to be conducted by the council's internal auditors (SIAP).[3]

2.2 The audit and position statement raised observations and added suggestions, and during the first year of the new Strategy further feedback has been received by councillors and officers. All feedback has been recorded by officers and assessed as part of this year's review of the Strategy. Key updates are noted below.

3 Information related to Recommendation 1: Summary of revisions made

3.1 The revisions made in Appendix 1 largely relate to clarifying different elements of the Strategy and improving its readability by adjusting its format. The revisions are as follows:

3.1.1 Separating the core of the strategy from those elements that provide guidance. This includes removing the previous Annex 6 – Continuous improvement, as it has become redundant as the Strategy has been in place for over a year and will be reviewed annually by officers.

3.1.2 Section 5: Added a paragraph explaining that high risks may be present, and that they may not be able to be lowered given the council's limited resources.

3.1.3 Section 7: Further information on how the Strategic Management Team, Corporate Management Team, Heads of Service and Project Boards review and escalate risks. This information is now also referenced in Section 4.

3.1.4 A new Section 8 has been added, which outlines how the council will deliver the Strategy. This includes incorporating the previous Annex 5 (Risk Management Culture) in this section.

3.1.5 Annex 1: Some minor changes have been made to the column descriptors in the risk register template, including the source of assurance for mitigations.

3.1.6 Annex 2: Further guidance added to financial impact guidance, and "environmental" and "health and safety" risk categories added.

3.1.7 Annex 4: Minor amendments made which signpost readers to the relevant persons/teams to approach for risk management training.

3.2 These recommendations address most of the feedback received on the current Strategy, since its approval last year. Two outstanding items for further consideration are outlined in the next section.

4 Information related to Recommendation 2: Consideration of risk appetite and risk targets

4.1 **Risk appetite:** at present, the council has a general risk appetite (see Section 5, page 9 in Appendix 1), which applies to all its activities. However, feedback on the Strategy suggests that the council could expand the breadth of its risk appetite, say by having different risk appetites for different groups of council activities.

4.2 For instance, if the council wishes to be more risk eager with revenue generating activities at its venues, a more eager risk appetite may be acceptable. Yet for macro-budget issues, the general cautious appetite would be appropriate, given the council's responsibility to safeguard public money and ensure that people who live, work and study in the Borough do not pick up the cost of failed council projects or mismanagement of funds.

4.3 The potential benefit of having more than one risk appetite, rather than one general appetite, could be that the council's appetite to risk is considered in more detail and better tailored towards specific business activities.

4.4 **Risk targets:** further consideration could also be given to introducing 'risk targets', i.e., a target risk score for each risk.

4.5 For example, the risk score for not submitting a report on time could be 8 (amber), which is acceptable. Yet a target risk of 3 (green) could be set, with the intention that the council will proactively seek to lower the existing score (8) to the target value (3), in order to further mitigate the risk to match the council's ambitions regarding timely report submissions.

4.6 The potential benefit of setting and working towards risk targets could be that by doing so, the council would be prompted to clearly set out the resources it is willing to deploy to treat a given risk, or whether tolerating it at its current level is acceptable.

4.7 **Possible next steps:** If the Committee is interested in pursuing these aspects of risk management in more detail, then further discussions outside of committee meetings would be beneficial. Therefore, officers could arrange a workshop with councillors to help guide discussions and capture the council's ambitions for risk management. Outcomes from the workshop would contribute to next year's review of the Strategy.

5 Risk Assessment

Legal or other duties

5.1 Equality Impact Assessment

5.1.1 There are no direct equality impacts arising from this report.

5.2 Crime & Disorder

5.2.1 There are no direct crime and disorder impacts arising from this report.

5.3 Safeguarding

5.3.1 There are no direct safeguarding implications arising from this report.

5.4 Dependencies

5.4.1 There are no significant dependencies connected to this report, although the council's approach to risk management does permeate all aspects of its governance, operations and strategic development.

5.5 Other

5.5.1 Not applicable.

6 Financial Implications

6.1 There are no direct financial implications. Any training and risk management develops put forward in this report are expected to be completed as part of business as usual activities.

6.2 **Section 151 Officer's comments**: None arising from the contents of this report.

7 Legal Implications

7.1 There are no direct legal implications arising from this report.

7.2 **Legal Officer's comments**: None arising from the contents of this report.

8 Policies, Plans & Partnerships

8.1 **Council's Key Priorities**: The following Key Priorities are engaged: Effective Council

8.2 **Service Plans**: The matter is included within the current Service Delivery Plan.

8.3 **Climate & Environmental Impact of recommendations**: There are no direct implications arising from this report.

8.4 **Sustainability Policy & Community Safety Implications**: There are no direct implications arising from this report.

8.5 **Partnerships**: Not applicable.

9 Background papers

9.1 The documents referred to in compiling this report are as follows:

Previous reports:

- [1] For the 2021-2022 audit of risk management see, EEBC (2022) Internal Audit Progress Report 2021-2022, 14th June, pp. 7-8. Online available: https://democracy.epsom-ewell.gov.uk/documents/s23874/Appendix%201%20Internal%20Audit%20Progress%20Report.pdf [last accessed 10/08/2023].

- [2] EEBC (2022) *Risk Management Strategy*, Strategy and Resources Committee, 26th July. Online available: https://democracy.epsom-ewell.gov.uk/documents/s24277/Appendix%201%20-%20Risk%20Management%20Strategy.pdf [10/08/2023].

- [3] For the SIAP position statement on the Risk Management Strategy see, EEBC (2022) *Internal Audit Progress Report 2022-2023 (November 2022)*, 17th November, pp. 8-9. Online available https://democracy.epsom-ewell.gov.uk/documents/s25119/Appendix%201%20-%20Internal%20Audit%20Progress%20Report%202022-2023%20November%202022.pdf [last accessed 10/08/2023].

Risk Management Strategy

Version number: 2.2
Date: September 2023

Version control

No.	Changes made	Date	Author	Approved by
1.0	Risk Management Strategy 2017-2021	15/11/2016	Head of Policy, Performance & Governance	Audit, Crime & Disorder Committee
2.0	Full strategy review. Draft strategy for approval by Strategy & Resources Committee.	25/03/2022	Business Assurance Manager	Strategic Management Team
2.1	Approved by committee with minor amendments to pp. 9, 15.	26/07/2022	Business Assurance Manager	Strategy & Resources Committee
2.2	Annual review, amendments to structure, and clarifications in S.5 (roles/responsibilities), S. 6 (high risks), S. 9 (delivery of the strategy), Annex 1 (register template), Annex 2 (financial impact criteria).	15/8/2023	Business Assurance Manager and Performance & Risk Officer	

Contents

Introduction

Risk is defined as an uncertain event or set of events which may, should they occur, affect our ability to successfully achieve our vision and objectives.[1]

Risk management is about managing opportunities and threats to objectives, and in doing so help create an environment of "no surprises".

Effective risk management requires a process of identifying, measuring, managing and monitoring risks. It is essential that risks are challenged and frequently reviewed.

The document is split in to two parts, the first describes the Council's strategy for managing risk and the second provides guidance to those involved in the day-to-day process of managing the Council's risks.

Part One – Council Strategy

1. Our risk management objectives

Our core aim is to adopt best practice in the identification and management of risks, for a Borough Council of our size and budget, and ensure risks are reduced to an acceptable level.

Risks will always exist, and we will not be able to eliminate them completely. Yet the effective management of risks will help enable the Council to remain sustainable in an environment of increasing budgetary pressures and service demand, changes in technology, legislation and our communities, and increased involvement with other organisations.

Therefore, this strategy's objectives are to:

- Raise awareness of risk and the need for risk management by all those connected with the delivery of the Council's corporate priorities.
- Provide the basis for a comprehensive yet simple framework which will integrate risk management into the culture of the organisation.
- Use risk management to strengthen our governance in all areas, such as decision making, service delivery, corporate planning, investments, and project management.
- Support the Council in anticipating and responding to changes in its social, environmental, and legislative environment.
- Help minimise injury, damage, loss and inconvenience to residents, staff, service users and assets arising from or connected with the delivery of our services.

[1] See our Corporate Plan 2020-2024 for more information, available online: https://www.epsom-ewell.gov.uk/council/four-year-plan.

- Continually improve our procedures for identification, assessment and management of risk in a cost-effective manner.

While a risk management strategy can engender the objectives above, it is notable that risk assessments are often largely qualitative judgements based on historical data, past experience and expert knowledge. Therefore, risk management has limitations and should not be the sole basis on which decisions are made. Yet at the most basic level, having a strategy of this kind will help invoke a healthy discourse on the risks that we face, both when looking internally at our services and governance, or when looking externally at the environment in which we operate.

2. Our approach

We need to identify and assess the risks that could hinder our ability to deliver our strategic objectives[2] and the provision of high-quality services to our residents and businesses.

To do this, we adopt the following process to manage risks:

1. **Risk identification**: this is the process of determining what might prevent us from achieving our objectives. Risks can be identified from various sources such as: strategic planning; monitoring our performance indicators; changes to our operating environment and horizon scanning; organisational forums such as management teams, project boards and committees; and risks identified via our internal audit function.

[2] See our Corporate Plan 2020-2024 for more information, available online: https://www.epsom-ewell.gov.uk/council/four-year-plan.

2. **Risk assessment**: once a risk has been identified, we then assess how likely it is to occur, and what impact it will have on our objectives if it did occur (e.g. what would be the consequences). We use a risk scoring matrix and risk registers to facilitate our assessments.[3]
3. **Risk response**: this involves taking actions to mitigate and control the risk. Essentially the aim of controls are to minimise, as far as is possible and proportionate, the risk from occurring.[4] The appropriate responses are considered in the context of the Risk appetite referred to in Section 5 below.
4. **Risk reporting**: this involves regularly reviewing our risks, at different levels of the organisation, to ensure our management of risk remains effective. For more information on this see Section 4.

This process applies to our existing service activities, and also when we enter new partnerships, embark on new projects, or when a new contract is being procured.

3. Our risk management structure

We adopt the three lines of defence approach as follows:

1st line: Managers and risk owners managing their risks.

2nd line: Corporate functions overseeing risk management e.g. divisional boards, Corporate Assurance, Strategic Management Team and policy committee risk registers.

3rd line: Internal audit, providing an independent and objective assessment of the council's risk management.

In addition, we classify risks in three levels to ensure there is a clear route of escalation should risks require additional support to manage.

The three risk levels are:

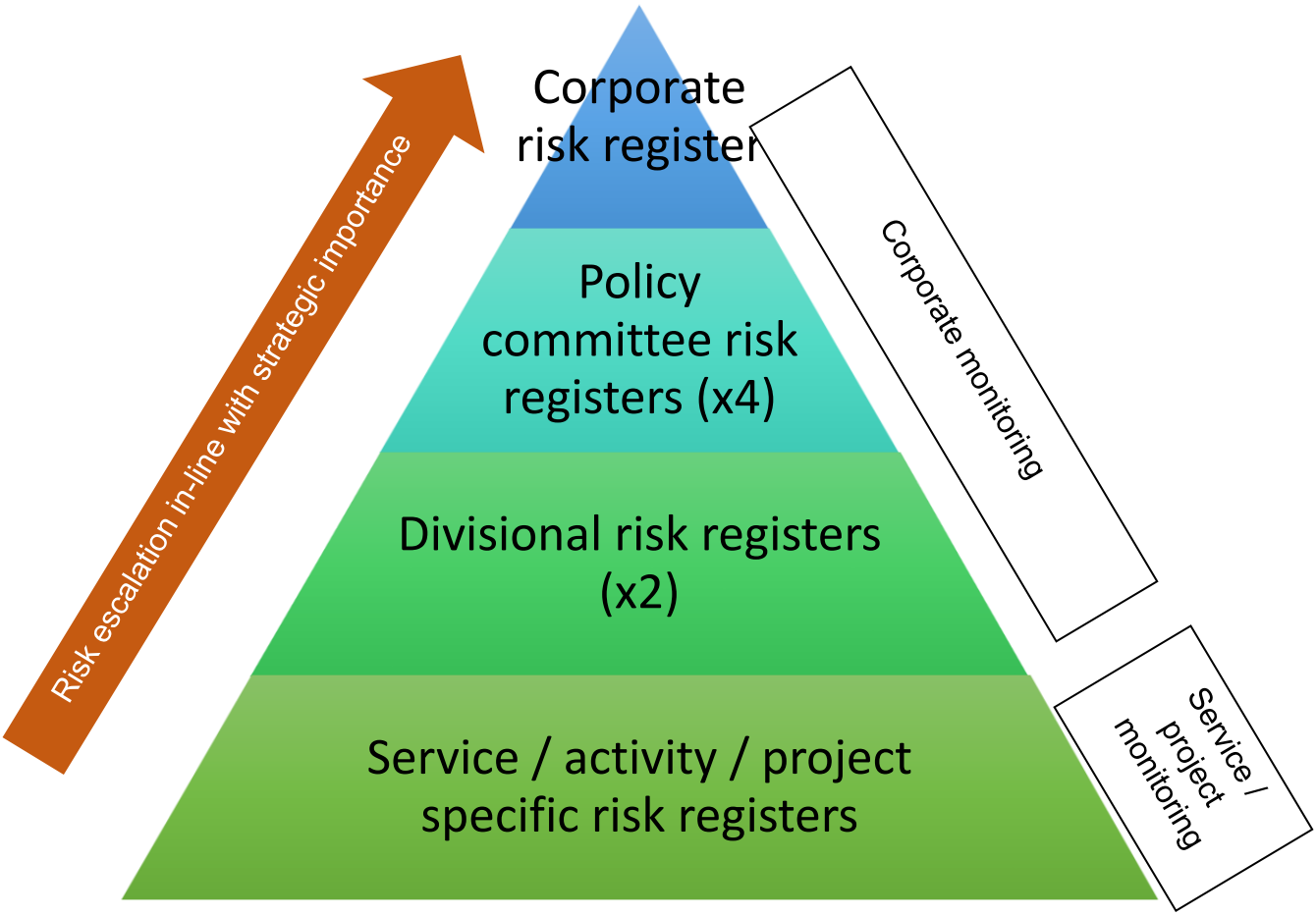
- **Corporate:** Strategic risks that could, if they are realised, have a significant detrimental effect on our ability to achieve our key objectives and delivery of core services. Notably, these risks span the organisation and our committees.
- **Committee:** These risks are similar to those at the corporate level with respect to their strategic importance. However, rather than spanning the

[3] See Annex 1 and Annex 2 for more information.
[4] For more information on risk responses, see Annex 2 – Risk Assessment Guidance.

whole Council, these risks relate to a particular committee's purview and can be effectively managed within its boundaries. If the risk becomes unmanageable or rises in strategic importance, it will be escalated to the corporate level.

- **Divisional:** Risks at this level are more operational and service based. These risks are still important for officers to manage, especially from a good governance perspective, but lack the strategic relevance to be included in the levels above. However, if the strategic importance of these risks rises, they will be escalated to the committee level. In some instances, a number of related individual risks at this 'level' may be aggregated to form a single risk that is more appropriately reviewed at the Committee or Corporate level.

The diagram below illustrates how these three levels of risk are arranged by their respective risk registers and included in our second line of defence. The arrow shows the route of escalation for risks that rise in strategic importance. The lowest level of the pyramid highlights that there may be a need for more operational-based risk registers, such as those related to specific projects, services or business activities. These risk registers will be monitored by the relevant manager (first line of defence).



4. Our roles and responsibilities

The table below highlights our key risk roles and responsibilities. See also Section 7 'Our Monitoring and Reporting arrangements.

Risk owners	• Day to day management of, and responsibility for specific risks. • Provide risk updates and escalate as necessary.
Heads of Service and project boards	• Own, review and quality assure thier Service specific risks / project risk registers. • Escalate and seek further support with risks as necessary.
Strategic Management Team	• Own, review and quality assure the corporate risk registers. • Champion risk managment. • Hold risk owners accountable.
Strategy & Resources Committee	• Own, review and approve the Risk Management Strategy.
Audit & Scrutiny Committee	• Scrutinise the application of the Risk Management Strategy and the corporate risk register. • Raise risk queries with relevant policy committee chairs.
Policy committee Chairs & Members	• Review performance and risk information, feedback to committees, SMT lead and relevant Head of Service; and respond to risk queries raised by the Audit & Scrutiny Committee.
Internal Audit	• Periodically review and assess the Council's risk management framework and procedures from an independent and objective standpoint.

5. Our risk appetite

Risk appetite involves continuously assessing the nature and extent of the risks an organisation is exposed to, and considering the amount of risk it is willing to take to achieve its objectives in the pursuit of stakeholder value.[5]

In our context, risk appetite is an expression of how much risk the Council is willing to accept in the pursuit of its objectives, such as delivering value for money services and projects for residents and businesses.

Risk appetite can be expressed differently for different business activities or categories of risk. For instance, an organisation may be eager to take risks in service transformation activities, but averse to reputational risks.[6]

The Council's overall risk appetite can be described as cautious: we have a duty to manage public money responsibly and deliver value for money. We are willing to consider all options when planning and making decisions. However, our preference is for low-risk options, although we will tolerate medium risks if sufficient controls and mitigations are in place and there is a high likelihood of delivering tangible benefits to our community.

Normally we will not take risks assessed as being high, following the application of mitigations and controls. We recognise that there may be some instances where a residual risk remains 'high' largely due to circumstances outside of the control of the Council such as through external financial instability. When residual risks have been assessed as 'high' we encourage managers to make clear when they are being tolerated and to explain why. Appetite can also be expressed in the table below, which shapes our planning and decision making.[7]

Risk rating	Residual risk assessment	Appetite response
High	12-16	Unacceptable level of risk exposure which requires urgent action.
Medium	4-9	Acceptable level of risk but requires action and active monitoring to manage the risk.
Low	1-3	Acceptable level of risk based on standard operational controls. Some risks, i.e. assessed at a 1 or 2 scoring, may not require mitigations.

[5] HM Government (2021) *Risk Appetite – Guidance Note*. Government Finance Function, p.3. Online available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/929385/Risk_Appetite_Guidance_Note_v1.0_FINAL.pdf [Last accessed 26/04/2022].
[6] For further examples and risk appetite scales see: HM Government (2021) *Risk Appetite – Guidance Note* (fn. 6), pp. 13-14, 17-19.
[7] This should be viewed in conjunction with the risk scoring matrix below in Annex 2.

6. Our risk assessment process

Once we identify a risk it is then assessed. In assessing a risk we consider the **likelihood** of the risk occurring, and if the risk were to be realised, what the **impact** on the Council would be.

We categorise likelihood on a scale of 1 to 4, one being **remote** and four being **very likely**. Impact is also categorised on a 1 to 4 scale, with one being **insignificant** and four being **severe**.

We score every risk twice: firstly, on its **inherent risk**, i.e. the risk with no mitigations / controls in place; and secondly the **residual risk**, i.e. the risk score **after** mitigations / controls have been applied.[8]

7. Our monitoring and reporting arrangements

Risk management monitoring and reporting occurs via various means in the Council, namely risk registers,[9] committee reports and divisional assurance statements. These mechanisms, along with the review of this strategy, help ensure there is robust oversight of risk management.

Policy committees

Each policy committee Chair reviews, and quality assures, their own committee risk register. We plan to also submit these as part of the corporate performance report to Audit & Scrutiny committee for additional oversight.

Furthermore, committee reports perform a key role in decision-making at the council, helping ensure Councillors have all the information they require when making decisions and formulating council strategy.

We use a standard template for every committee report. There is a “Risk assessment” section, where report authors can list all key risks relevant to the report and the decisions Councillors are considering. In some cases, such as reports that include options appraisals, the risks may be included within the main body of the report where each option is presented.

Strategic Management Team and Corporate Management Team

SMT and CMT review and quality assure the corporate risk register every quarter: for SMT, this occurs via the committee reports process where the Audit & Scrutiny Committee performance report is reviewed ahead of the committee meeting during an SMT meeting; for CMT, the corporate risk registers are reviewed at one of their monthly meetings each quarter, via the ‘Committee Business Pack’.

[8] See Annex 1 for an example of this way of scoring, and for scoring guidance Annex 2.
[9] See Section 3.

Heads of Service

Each Head of Service initially reviews their corporate, committee and divisional risks with their managers, which are signed off with the Business Assurance team on a quarterly basis. Any significant updates (e.g. a risk moving from amber to red), and escalations (e.g. a risk moving from the 'committee' to 'corporate' level) are raised and discussed with the appropriate Director during their Divisional Management Team meetings (or in separate meetings if required).

Project boards

The project manager, in consultation with the project sponsor or standalone project board, will regularly review and quality assure the project risk register. They report monthly to the Corporate Project Board (CPB), any significant risk updates or escalations. The CPB will then provide feedback to the project manager following their monthly meeting.

Divisional assurance statements

Assurance for corporate risk management is also gained via Divisional Assurance Statements. Each Head of Service acknowledges and confirms their responsibility for risk management within their service.

Internal audit

Our internal audit function will specifically review the effectiveness of the Council's risk management periodically. They will also raise risk observations as part of every audit report.

8. How we will deliver the strategy

Achieving our risk management goals and objectives relies on people supporting and contributing to them. Therefore, we will:

- Embed risk management in our organisational culture, via induction processes, corporate reporting, and the annual review of this strategy (with associated briefings). Measured by risk KPIs (see below).
- Ensure all colleagues, especially risk owners, understand their roles and responsibilities for risk management. We will do this by sharing this strategy via staff updates, publishing on E-Hub and 'members news'. We also offer e training through activities such as introductory workshops to all Heads of Service, one-to-one sessions for managers and other risk owners, and sessions for councillors. These help enable knowledge dissemination and develop individuals' capability to manage risk. Directors will also review risk management with their Heads of Services at Divisional meetings, 1-2-1s and

Corporate Management Team meetings.[10] Measured by risk KPIs (see below).

- Review our corporate plan, and meaningfully consider risk in decision-making, service delivery and project management. Measured by consideration of risk featuring in development and performance monitoring of our Four-Year Plan, via engagement with both officers and councillors, and embedding risk management principles in corporate project toolkit. Also, continuing reviews of risk registers at Corporate Management Team, committee policy Chairs, and Corporate Project Board meetings.
- Corporately monitor the effectiveness of our risk management arrangements and share our results with the Audit & Scrutiny Committee, via the corporate performance reports and the Annual Governance Statement. Feeback on the strategy via the annual review of this strategy.
- Review our corporate risk register quarterly and report and interrogate risks as necessary, through the arrangements described in Section 7 Measured by standing quarterly agenda item to review risks for CMT, Audit and Scrutiny committee reports process and policy committee Chairs meetings.
- Welcome and actively seek regular independent review of our risk management framework and practices by internal and external audit.[11] Measured by the number of reviews carried out over a two-year rolling period.

Risk key performance Indicators (KPIs)

To support delivery of our Risk Management Strategy officers will periodically monitor the awareness and pro-active engagement of staff in managing risk through the following KPIs.

1. The number of individuals completing related e-learning.
2. The number of workshops and one-to-one ‘risk’ sessions held during the year.
3. The number of risk management related briefings released each year (e.g. staff updates).

[10] See Section 7.
[11] Audit Scotland (2021) *Risk Management Framework, v.March2021. Scotland: Edinburgh*.

Part Two - Guidance

The following annexes contain guidance information to assist with the delivery of the strategy.

Annex 1 – Example risk register

Example restaurant risk register

ID.	Risk Identified	Risk Consequences	Risk Owner	Likelihood	Impact	Inherent Risk TOTAL	Mitigations & Controls in place Source of assurance, I = internal, E= external	Likelihood	Impact	Residual Risk TOTAL	Direction of travel Compared to previous quarter	Commentary and future actions to further mitigate risk
1	Canteen revenue decreases due to limited ice cream flavours	* Negative impact on service's revenue. * Negative impact on service's reputation.	Canteen Manager	**3**	**3**	**9**	* Monthly customer review of ice cream menu. (E) * Equipment purchased that enables current ingredients to be mixed to create four more flavours. (I)	**2**	**3**	**6**	**Worsened** *(Risk score increased since last review)*	* Apply for grant funding for research and development into new flavours. [*Not being pursued at present as would require an additional staff member to write, submit and fulfil the bid criteria*]
2	Cannot process payment transactions quickly due to system limitations	* Long queues form at peak times. * Poor service to customers, leads to reduced custom.	Canteen Manager	**4**	**3**	**12**	***** Additional system processing capacity purchased. (I) * System maintenance contract (E)	**1**	**3**	**3**	**Improved** *(Risk score lowered since last review)*	* None at present.
3	No seats available for customers at peak times due to size of the canteen.	* Reduction in demand as customers purchase lunch from other nearby restaurants that have seating.	Canteen Manager	**4**	**3**	**12**	* Signage in place which notifies customers of peak times and encourages them to visit off-peak. (I)	**3**	**3**	**9**	**No change** *(Risk score unchanged since last review)*	* Extend the canteen seating area. [Scoping exercise commissioned].

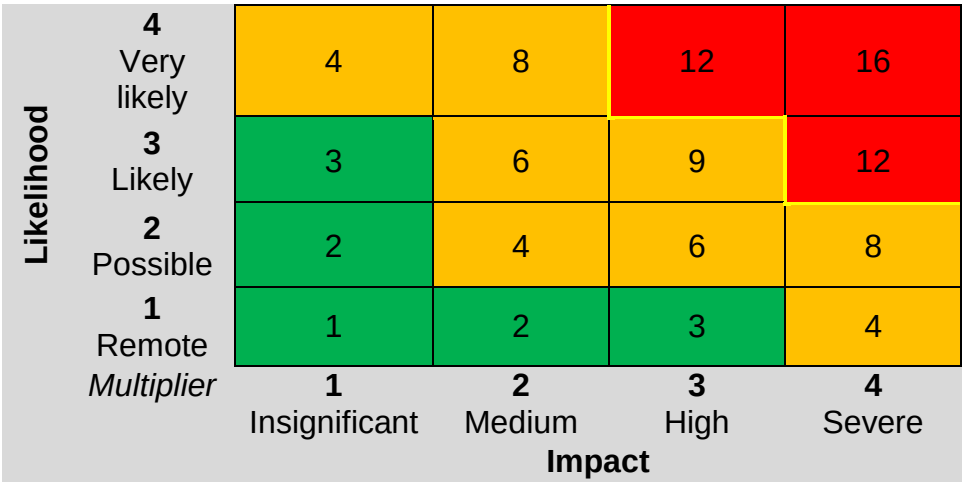
Annex 2 – Risk assessment guidance

Risk assessment involves looking at the impact a risk could have, and the likelihood that it will arise. Multiplying the impact and likelihood scores provides the total risk score. As Annex 1 shows, risks are scored both on their inherent risk, i.e. the risk with no mitigations / controls in place, and the residual risk, i.e. the risk score after mitigations / controls have been applied.

Step 1: Score the **inherent** risk = *impact x likelihood (with no controls)*

Step 2: Score the final **residual** risk = *impact x likelihood (with controls).*

Step 3: Review final risk score against the **risk tolerance boundary** (yellow line). If High (red), seek to further treat / transfer to reduce to Medium (amber) or Low (green).



Key

Red	High risks
Amber	Medium risks
Green	Low risks
Yellow	Risk tolerance boundary

Likelihood criteria

Risk likelihood	Description
Remote (1)	May occur only in exceptional circumstances (0%-15%)
Possible (2)	Could occur at some time (>15%-40%)
Likely (3)	Will probably occur in most circumstances (>40% to 80%)
Highly likely (4)	Expected to occur in most circumstances (>80%)

Impact criteria

The table below is guidance and therefore not exhaustive nor definitive. Fields can cross-pollinate: for example, when looking at an impact on corporate objectives, the risk owner may also want to consider the financial impact to form their judgement. Further, the overall impact score for a risk should be weighted in favour of the highest score in any of the impact categories.

	Insignificant (1)	**Medium (2)**	**High (3)**	**Severe (4)**
Financial	Tier 1 – Less than 5% over budget OR Tier 2 – Corporate / Committee Thresholds Under £20,000	Tier 1- 5-10% over budget OR Tier 2 – Corporate / Committee Thresholds £20,000 - £49,999	Tier 1- 10-15% over budget OR Tier 2 – Corporate / Committee Thresholds £50,000 - £99,999	Tier 1 – More than 15% over budget OR Tier 2 – Corporate / Committee Thresholds Over £100,000
Service	Short term service disruption	Noticeable service disruption affecting customers	Significant service failure but not directly affecting vulnerable groups	Serious service failure directly affecting vulnerable groups
Reputation	Contained within business unit / service	Short term negative local media attention	Significant and sustained negative local media attention and national media attention	Sustained negative national media attention
Injury or illness	Minor injury, or illness, first aid, no days lost	Minor injury, or illness, medical treatment, days lost	Moderate injury, medical treatment, hospitalisation, <14 days lost, RIDDOR reportable	Fatality, extensive injuries, long-term illness (>14 days)
Staff	Loss of staff morale but unlikely to	Increasing staff dissatisfaction;	Adverse staff dissatisfaction /	Significant staff dissatisfaction/

	result in absence or turnover of staff	Isolated instances of behaviours outside of value framework	likely increased absence and turnover of staff; Negative impact on culture & value framework	increased long-term absence & staff turnover; Loss of culture and value framework
Corporate objectives	Negligible impact on RAG status	RAG status increased to amber for 1-3 months	RAG status changed to amber for 3-6 months	RAG status increased to amber for > 6 months or to red
Regulatory & legal	Minor civil litigation and / or regulatory breach	Major civil litigation and / or local public enquiry. Regulatory breach that does not require external reporting.	Major civil litigation and / or national public enquiry. Breach that requires reporting to external body / regulator.	Legal action certain, leading to Section 151 or government Intervention, or criminal charges. Breach that reflects systemic failures. Or Statutory requirement to deliver a service
Business continuity	Up to date and exercised business continuity plan in place	Up to date plan, not exercised, in place	Out of date plan in place	No plan in place
Asset loss	Minor damage to single asset	Minor damage to multiple assets	Major damage to single or multiple assets	Significant > complete loss of assets
Project delivery[12]	Minor delay to Project, no impact on benefits realisation	Significant delay to project and / or moderate impact on benefits realisation	Project delay impacts on a business unit's Performance and / or significant impact on	Project delay impacts the Council's performance and / or corporate

[12] For project cost risks, see and use "Financial" row.

			benefits realisation	objectives, and / or benefits fail to be realised
Intervention required	Intervention by Service Manager, Project Manager or equivalent	Intervention by Head of Service	Intervention by Strategic Management Team, Corporate Board or equivalent; notify Members.	Intervention by Members, S151 Officer

Risk responses

Risk responses can be categorised into the 4 T's:

- **Terminate**: in this situation the risk is terminated by deciding not to proceed with an activity. For example, if a particular project is very high risk and the risk cannot be mitigated it might be decided to cancel the project. Alternatively, the decision may be made to carry out the activity in a different way.
- **Transfer**: in this scenario, another party bears or shares all or part of the risk. For example, this could include transferring out an area of work or by using insurance.
- **Treat**: this involves identifying mitigating actions or controls to reduce risk. These controls should be monitored on a regular basis to ensure that they are effective.
- **Tolerate**: in this case, it may not always may be necessary (or appropriate) to take action to treat risks, for example, where the cost of treating the risk is considered to outweigh the potential benefits. If the risk is shown as 'green' after mitigating actions, then it can probably be tolerated."[13]

Risk level

Risk managers should consider which of the three risk levels apply i.e. Corporate, Committee or Divisional / Service as detailed in Section 3 of the Strategy.

[13] Audit Scotland (2021) *Risk Management Framework, v.March2021. Scotland: Edinburgh*

Annex 3 – Risk categories

The risk categories below are included in this strategy firstly, to aid the identification of risks by outlining a range of areas where risks can arise. Secondly, risk categories help build a picture of the current risk environment, by revealing particular areas of risk that may be prevalent at a moment in time.

For instance, if several services report risks around interacting with residents, businesses and customers, it may be that there is a general move towards a more technology enabled group of Council stakeholders, which requires the Council to update its ICT systems to enable customers to interact with the it via digital platforms.

The categories are not intended to be exhaustive or prescriptive but help guide officers and Members when managing risk.

Categories:

- **Customer/Citizen** – risks associated with failing to meet the changing needs and expectations of our residents and businesses, including the effects of wider socio-economic changes.
- **Financial** – risks related to the Council's financial planning and budgetary pressures, meeting our financial commitments, investments and the adequacy of our insurance cover. Where possible the financial risk should be quantified in relation to the relevant policy committee threshold.
- **Fraud** - Risks arising from intentional deception to secure unfair or unlawful gain against the Council, or to deprive the Council of its legal rights.
- **Governance** – risks that relate to a weakening of the Council's systems of internal control and governance.
- **Legal** – risks that may arise due to changes in legislation, ~~or~~ possible breaches of existing legislation, or statutory duty to deliver a service.
- **Operational** – risks that relate to the efficient, safe and cost-effective running of our services.
- **Partnership** – risks related to an arrangement with a third party to deliver the Council's services. This could include the performance, cost and quality of a contractor's service delivery.
- **Project** – risks associated with the delivery of the Council's corporate programmes and projects.
- **Reputational** – risks that will potentially damage the public's perception of the Council by failing to meet stakeholder expectations.
- **Strategic** – risks associated with the Council achieving its strategic objectives, such as those in the Four-Year Plan and annual plans.

- **Environmental** – risks of harm or danger to the environment for example from natural hazards, pollution or depletion of natural resources, and specifically those in opposition to our Climate Change Strategy.
- **Health and Safety** – risks arising from failure to comply with health and safety legislation and industry best practice.

Annex 4 - Training

Councillors

- Risk management training provided to councillors will include contextualising risk management in terms of a council of Epsom and Ewell's size and our risk management strategy. Councillors should approach the Head of Policy and Corporate Resources if they are interested in attending this type of training.

Officers

- Risk management e-learning available to all managers, project managers and other risk owners.
- In-house workshops on the Strategy are available for all managers, and other risk owners (as nominated). This could include one-to-one sessions as requested by managers, which can take place at any time throughout the year as necessary. Officers should contact the Business Assurance Manager to arrange this training.

This page is intentionally left blank