EPSOM & EWELL BOROUGH COUNCIL

Risk Management Strategy

Version number: 2.0
Date: July 2022

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

Contents

1. 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.

1.1. 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.
- 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

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

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. Risk Management Framework

2.1. 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. **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]

[2] See our Corporate Plan 2020-2024 for more information, available online: https://www.epsom-ewell.gov.uk/council/four-year-plan.
[3] See Annex 1 and Annex 2 for more information.

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]
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.

2.2. 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.

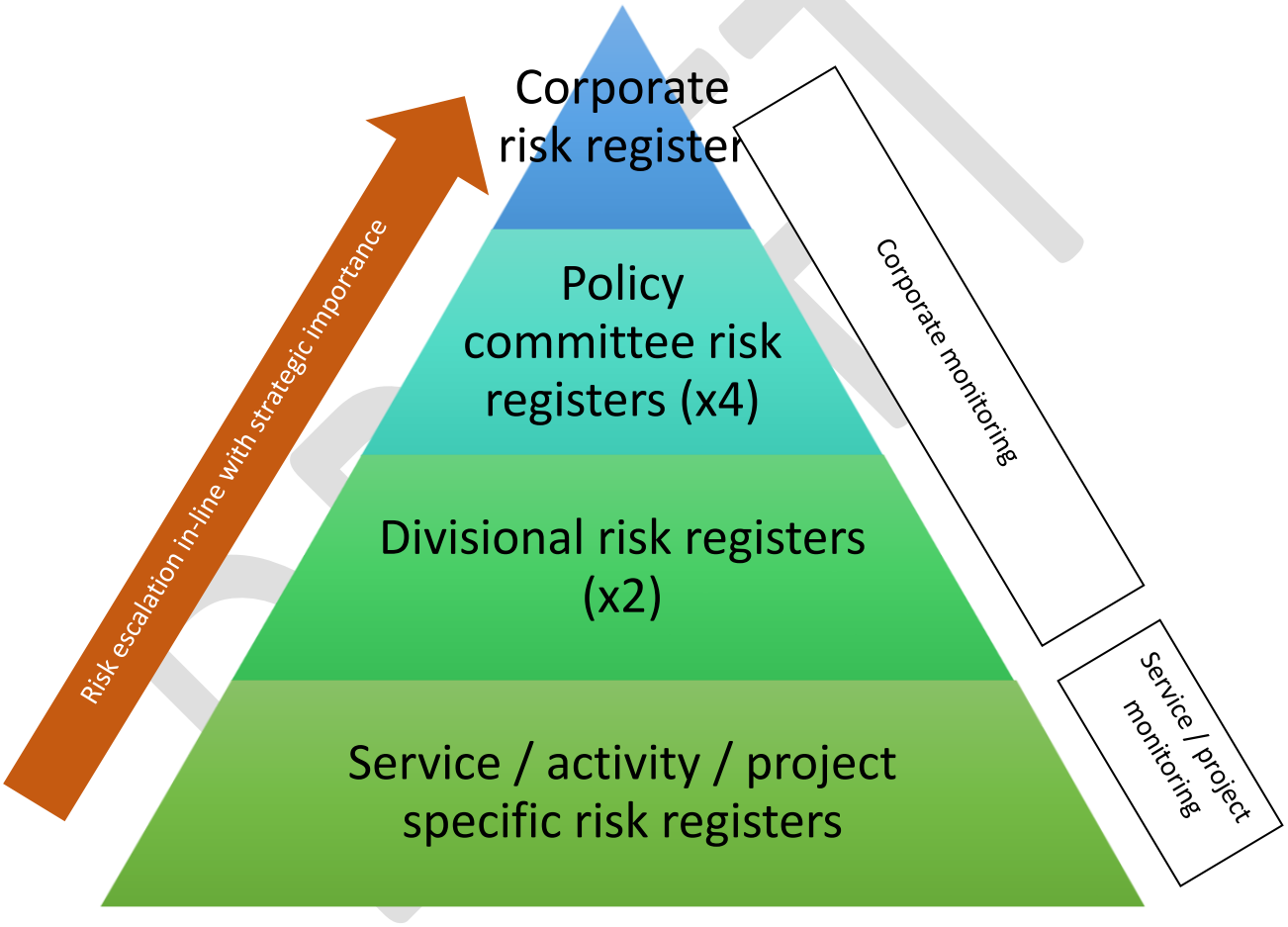
The three risk levels are:

- **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 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 / Service:** Risks at this level are more operational and service based. These risks are still important for officers to manage, especially from a

[4] For more information on risk responses, see Annex 2 – Risk Assessment Guidance.

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.

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).



2.3. Roles and responsibilities

The table below highlights our key risk roles and responsibilities:

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 specific divisional / project risk register. • Escalate and seek further support with risks as necessary.
Strategic Management Team	• Own, review and quality assure the Corporate Risk Register. • Champion risk managment. • Hold risk owners accountable.
Strategy & Resouces 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 issues and concerns 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 formally respond to enquiries from Audit & Scrutiny Committee.
Internal Audit	• Periodically review and assess the Council's risk management framework and procedures from an independent and objective standpoint.

3. Risk Assessment

3.1. 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. Therefore, we will not take risks assessed as being high, following the application of mitigations and controls. 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.

Our 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 Section 3.2.

3.2. Risk analysis and assessment

Once a risk is identified it is assessed. Assessing a risk involves considering the **likelihood** of the risk occurring, and if the risk were to be realised, what the **impact** on the Council would be.

Likelihood is categorised 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**.

Every risk is scored 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]

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).

Likelihood					
	4 Very likely	4	8	12	16
	3 Likely	3	6	9	12
	2 Possible	2	4	6	8
	1 Remote	1	2	3	4
	Multiplier	**1** Insignificant	**2** Medium	**3** High	**4** Severe
		Impact			

Key

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

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

4. 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.

4.1. Policy committees

Each policy committee reviews, and quality assures, its own committee risk register. These are submitted 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.

4.2. 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.

4.3. 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.

[9] See Section 2.2.

Annex 1 – Example risk register

Example restaurant risk register

ID.	Risk Identified	Risk Consequences	Risk Owner	Likelihood	Impact	Inherent Risk TOTAL	Mitigations & Controls	Likelihood	Impact	Residual Risk TOTAL	Direction of travel	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 review of ice cream menu. * Equipment purchased that enables current ingredients to be mixed to create four more flavours.	**2**	**3**	**6**	↑ *(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.	**1**	**3**	**3**	↓ *(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**	* Put signage in place which notifies customers of peak times and encourages them to visit off-peak.	**3**	**3**	**9**	↔ *(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.

Total risk score = likelihood *x* impact

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	Less than 5% over budget	5-10% over budget	10-15% over budget	More than 15% over budget
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,	Fatality, extensive injuries, long-term illness (>14 days)

			RIDDOR reportable	
Staff	Loss of staff morale but unlikely to result in absence or turnover of staff	Declining staff dissatisfaction; Isolated instances of behaviours outside of value framework	Adverse staff dissatisfaction / likely increased absence and turnover of staff; Negative impact on culture & value framework	Significant staff dissatisfaction/ 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.
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[10]	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 benefits realisation	Project delay impacts the Council's performance and / or corporate objectives, and / or benefits fail to be realise
Intervention required	Intervention by Service Manager, Project Manager or equivalent	Intervention by Head of Service	Intervention by Strategic Management Team, Corporate Board or	Intervention by Members, S151 Officer

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

			equivalent; notify Members.	

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."[11]

[11] Audit Scotland (2021): *Risk Management Framework*. Online available: https://www.audit-scotland.gov.uk/uploads/docs/um/risk_management_framework_2021.pdf, p.13 [Last accessed: 24/02/2022].

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.
- **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.
- **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.

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. This will be arranged following the adoption of this document.

Officers

- Risk management e-learning to all managers, project managers and other risk owners. This will be issued following the adoption of this document.
- Workshops for all Heads of Service, managers, and other risk owners (as nominated) on the strategy. This will include an offer of one-to-one sessions as requested by managers, which can take place at any time throughout the year as necessary.

Annex 5 – Risk management culture

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

- Embed risk management in our Councillor and officer induction processes, and via annual briefings.
- Ensure all colleagues, especially risk owners, understand their roles and responsibilities for risk management, by sharing this strategy and providing an introductory workshop to all Heads of Service and offering all managers one-to-one sessions, which will enable knowledge dissemination.[12]
- Review our corporate plan, and meaningfully consider risk in decision-making, service delivery and project management.
- Corporately monitor the effectiveness of our risk management arrangements and share our results with the Audit & Scrutiny Committee, via the review of this document and the Annual Governance Statement.
- Review our corporate risk register quarterly and interrogate risks as necessary.
- Welcome independent review of our risk management framework and practices by internal and external audit.[13]

[12] See Annex 4.

[13] Audit Scotland (2021): *Risk Management Framework*. Online available: https://www.audit-scotland.gov.uk/uploads/docs/um/risk_management_framework_2021.pdf, p.6 [Last accessed: 24/02/2022].

Annex 6 – Continuous improvement

This version of the risk management strategy includes several key updates to the previous version, such as a dual scoring approach to risk assessment, using a 4x4 scoring matrix and aligning our risk registers with the new organisational structure.

Therefore, our key aim for the next year is to embed these changes in the organisation, ensuring all managers are familiar with the strategy and feel confident in managing risk. This should enhance the consistency of our risk management across the organisation.