Runnymede Borough Council

Risk Management Framework 2023 - 2026

October 2023

Runnymede Borough Council

Contents

1. Purpose, aims and objectives of the Risk Management Framework

The Council's Risk Management Framework sets out the approach to holistic, cross-organisational risk management at both a strategic and operational level to fulfil the legislative requirements as laid down by the Local Government Act 1999 and Accounts & Audit Regulations 2015, to ensure effective and efficient corporate governance and reporting.

The aim of the framework is to formalise, embed and continuously improve processes and procedures for the identification and evaluation of risks and opportunities and the cost-effective control of risks to ensure that they are reduced to an acceptable level and any impact on delivery of objectives is minimised.

The scope of the framework covers both the corporate culture and processes and procedures to ensure risks are managed. It does not replace established risk assessment processes, for example, for health and safety compliance, business continuity or emergency planning, but instead builds on and supports those activities by establishing a consistent framework for their identification, assessment, and escalation, as required.

The risk management objectives of the Council are to:
- Embed and raise awareness of risk and opportunity management into the culture and corporate processes of the Council.
- Manage risk and opportunity in accordance with best practice and in particular in accordance with the requirements of the Annual Governance Statement.
- Assume legal compliance as an absolute minimum.
- Prevent injury and damage and reduce the cost of risk.

These objectives will be achieved by:
- Establishing and implementing a clear risk management process that is communicated to all officers and Members.
- Setting out the Council's risk appetite to ensure consistency in approach to risk management.
- Setting the tolerances for risk and the criteria for its mitigation and control.
- Clearly define roles and responsibilities for risk management.
- Providing risk management training to officers and members.
- Holding corporate and operational risk management sessions to identify risks.
- Ensuring that risks are identified and managed as part of the project management methodology and contract management framework.
- Maintaining and reviewing a register of corporate, operational, project and contract risks and opportunities and assigning ownership for each risk.
- Ensuring that reports to Service Committees, Standards and Audit Committee, Corporate Management Committee and Council include implications of any significant risks.
- Identifying risks and opportunities in relation to working in partnerships.
- Ensuring that the Standards and Audit Committee receive regular reports on the key business risks and opportunities and takes action to ensure that business risks and opportunities are being actively managed.
- Risk management being part of every staff member's competency framework, job description and annual performance review.

All staff and stakeholders involved in delivery of the Corporate Business Plan, Service Area Plans and business as usual activities have a responsibility to assess and manage risks and identify and apply learning from risks.

2. Risk Management Definition

The Corporate Business Plan 2022-2026 and the associated corporate strategies for Economic Development, Empowering Communities, Climate Change, Health and Wellbeing and Organisational Development provide the strategic direction and objectives to be delivered over the period of the plan. Annual service area plans set out the specific corporate and operational objectives that will be delivered by the teams and individuals in the service area over the following 12-month period.

A risk is an uncertain event or condition that, if occurs, has a positive or negative effect on delivery of these objectives whether at the operational or strategic level. A risk is something that may happen in the future.

Risk should not be confused with liabilities that are known events that already exist and which are subject to a different management process. The difference is that risks can be treated in a number of ways including financial risk transfer. Liabilities cannot - they are a known condition and are part of the opportunity cost.

For the purpose of this framework, risks that score above the threshold of 10 (See Step 3 Scoring Risk) after mitigation are escalated for consideration on the corporate risk register (CRR), with those risks scoring 15-25 after mitigation defined as 'significant risks'.

Risk management is the systematic process of identifying, evaluating, and managing those uncertainties and bringing them to an acceptable level. By doing this we safeguard our residents and colleagues while increasing the chances of our corporate and operational objectives being achieved, safeguard public money, and protect our reputation.

The Council's definition of risk management is:

"The iterative, systematic application of principles and processes to risk identification, assessment, management and on-going monitoring of risks and opportunities in pursuance of Council objectives."

3. Context of Risk Management in Local Government

The Council has a legal duty to have risk management arrangements in place, as stated in the Accounts & Audit Regulations 2015 (Part 2: Internal control - Responsibility for internal control):

"A relevant body must ensure that it has a sound system of internal control which:

(a) facilitates the effective exercise of its functions and the achievement of its aims and objectives.

(b) ensures that the financial and operational management of the authority is effective.

(c) includes effective arrangements for the management of risk."

The next few years will continue to present significant challenges for the Council in delivering services under increased economic pressures. The challenges will mean that the Council needs to adapt and change through discovering and implementing efficiencies, increasing income generation, utilising partnership-working or exploring alternative service delivery models. Whilst these changes create opportunities; they also create risk and uncertainty. As new ways of working emerge, the risk management process will need to adapt and respond to these.

3.1. Overview of Local Code of Corporate Governance

The Council has formally adopted a code of corporate governance as recommended in the CIPFA/SOLACE Framework Delivering Good Governance in Local Government 2016 edition.

The Council is committed to the principles and sub-principles of good governance identified within the International Framework and has reproduced these within its own local Code. These principles and sub-principles set out the actions and behaviours expected of the Council to ensure good governance is delivered in all that it does.

Of these, the Core Principle relating to risk is as follows:

F. Managing risks and performance through robust internal control and strong public financial management

The Council has also adopted the CIPFA Statement on the Role of the Chief Financial Officer (CFO) in Local Government which sets out the core responsibilities of the CFO, including development of the risk management framework and risk reporting.

3.2. Annual Governance Statement

Runnymede Borough Council is responsible for ensuring that its business is conducted in accordance with the law and proper standards, and that public money is safeguarded and properly accounted for, and used economically, efficiently, and effectively.

The Council also has a duty under the Local Government Act 1999 to secure continuous improvement in the way in which its functions are exercised, having regard to a combination of economy, efficiency and effectiveness. In discharging this overall responsibility, the Council is also responsible for putting in place proper arrangements for the governance of its affairs and facilitating the effective exercise of its functions, which includes arrangements for the management of risk.

Regulation 6 of the Accounts and Audit Regulations 2015 requires the Council to undertake an annual review of the effectiveness of its system of internal control, known as the Annual Governance Statement (AGS), which explains how it is complying with its Local Code of Corporate Governance including its processes for risk management. This annual review is an important element in ensuring that good governance and risk management underpin the delivery of Council services and that associated processes are relevant, up to date and effective.

3.3. Benefits of Risk Management in Local Government

Continuous improvement of cross-organisational risk management will enhance the delivery of benefits for the Council that include:

- Improved service delivery: resulting from fewer disruptions/enhanced controls.
- Increased probability of achieving strategic objectives: through minimising or removing key obstacles.
- Improved awareness of risk: the Council can be more robust in in taking advantage of new opportunities if incumbent risks are assessed and subject to active positive management.
- Improved corporate governance: through stronger, more transparent evidence-based decision making, accountability and prioritisation.
- Safeguard the organisation and provide assurance to all stakeholders such as elected members and residents.

3.4. Other related processes that identify risk

To support achievement of strategic and operational objectives (covered specifically in this framework) there are a number of additional and related activities that involve identification and management of risk. These include business continuity, emergency planning (provided by third party service provider, Applied Resilience), IT disaster recovery and Health & Safety compliance within the Council. It is important that the role and interrelationships of each are clearly understood if the Council is to effectively manage risk across the organisation and with external stakeholders and partners.

Separate policies and procedures exist to specifically support business continuity, emergency planning, IT disaster recovery and health and safety compliance.

Whilst this framework specifically addresses risk associated with delivery of corporate and operational objectives, the same escalation process is used for risk identified through business continuity, emergency planning, IT disaster recovery and Health & Safety compliance. Risks identified and assessed that score highly post-mitigation are escalated to Corporate Leadership Team (CLT) for consideration for inclusion on the corporate risk register.

Diagram: Relationship between Risk Management processes across the Council

ACTIVITIES	Horizon scanning and Risk Management at strategic and operational levels. Key policy documents e.g. Capital and investment strategy.	Business Continuity planning	Emergency planning	Disaster recovery	Health and safety compliance
PROCESS	Recognising risks facing the Council	Risks, that if materialise, may impact on service delivery	Significant crisis or emergency requiring response	Restoring data systems and applications	Health and safety compliance risk assessments
ACTORS	CLT SLT Project sponsors Contract Owners All staff Internal Audit	SLT (strategic Business Continuity Plan) Individual CHoS (service area Business Continuity Plans)	CLT SLT Applied Resilience	Digital Services Infrastructure team	HR/ H&S Officer (DSO) (workforce risk assessments) Compliance officers (3rd parties)

3.5. Partnership Risk Management

The Council recognises the important role and contributions its partners make to the achievement of the Corporate Business Plan and associated corporate strategies. Risk management plays a vital role in ensuring that these partnerships are successful and that they do not expose the Council to unnecessary risks.

Examples of partnership working include:

- Joint commissioning/provisioning with other public bodies
- Joint ventures with other public sector entities
- Partnership and joint ventures with the private sector
- Council companies, social enterprises and trusts

An example of partnership working and the opportunity that this has brought about is the Community Services Partnership between Runnymede and Surrey Heath Borough Council. As part of the process of setting-up, developing and managing partnerships, relevant risks must be identified, managed and monitored.

To improve monitoring and management of risk associated with partnerships, the corporate risk register will include significant risks associated with these delivery arrangements including business continuity risks. Corporate Heads of Service (CHoS) will identify and include these risks within their service area risk registers and escalate significant risks to the CLT for entry on the Corporate Risk Register.

4. Risk Management Framework

Identification and management of risk on a number of levels, mirrors the Council's 'Golden thread' ensuring that objectives set for the organisation and documented in the Corporate Business Plan and associated Corporate Strategies are translated and included in Service Area Plans and as a result in team and individual objectives for delivery. Assessment and management of risk also occurs at both the corporate strategic level, and at operational levels in service, project or contract risk registers.

Operational risks can lead to the success or failure of a corporate objective and therefore might inform the approach and decision making of senior management at both the service and corporate leadership levels. This approach supports a more holistic understanding of risk across the organisation.

Effective risk management also considers opportunities as well as threats to delivery of strategic and operational objectives.

4.1. Managing risk to deliver corporate and operational objectives.

Annually, as part of the Corporate Business and Budget Planning process, each service area identifies and puts forward key activities (project and non-project) to be undertaken and any revenue or capital budget growth required over the course of the coming financial year. Service areas are required to review service risk as well as horizon scan to include political, economic, sociological, technical, legal and environmental as well as other risks which become apparent in the risk landscape in which they operate. This can lead to identification of risks that require action to mitigate any impact that may occur if the risk were to materialise. These actions are then managed and delivered as part of the normal business of the service area throughout the project or year.

Every staff member has an annual performance review (appraisal) to assess and monitor progress against set objectives as well as setting objectives for the coming year to deliver Service Area Plan activities. As part of this, an awareness of risks and their management is cascaded down to staff through their objectives.

Risk management is undertaken within the Council through the following processes:

I. In addition to day-to-day management, teams carry out regular reviews of progress against their Service Area Plan, including an assessment of the Service Area Plan risk register.

II. As described within the project management methodology, an overview of the progress (including RAG status of project criteria) of all category 'A' and 'B' projects is provided monthly to the Chief Executive/ CLT and quarterly to the Corporate Management Committee. As part of this reporting process, overall project risk is rated, and senior leaders alerted to any project risks that require remedial action outside of project tolerances or escalated for consideration to be added to the Corporate Risk Register. Category 'C' projects are monitored within a service area and are reported to the Corporate Management Committee on a 6-monthly basis.

III. Each Corporate Head of Service (as members of the Senior Leadership Team (SLT)), provide an overview of service performance and emerging risks as part of the review of the Corporate Risk Register on a quarterly basis.

5. Risk Management Process

The monitoring and reporting of risks to the Council and its operations are as follows:

- As part of the annual business planning cycle, Corporate Heads of Service develop their service area risk register. Identification of risks may lead to necessary action to avoid, mitigate, or accommodate the risk and these activities will to be included in the Service Area Plan.

- Significant risks within these risk registers above a certain risk score are escalated to CLT for consideration of inclusion on the Corporate Risk Register. See **Appendix 1: Risk Escalation Process Diagram**

- On a regular and frequent basis, service area risk registers are reviewed by the Corporate Head of Service and team(s). Any changes to risks, existing and planned controls, progress against any related risk actions and risk ratings are updated on the register by the risk owners, as necessary. Significant risks above a certain risk score are escalated to CLT for consideration for the Corporate Risk Register.

- The CRR is reviewed on a regular basis by CLT and on a quarterly basis by SLT. This ensures all Corporate Heads of Service are aware of significant risks, and can collectively discuss the risks, and develop and plan mitigation. This provides a checkpoint to ensure that similar risks from across the organisation are being consistently scored. Review of organisation risk in this way can also identify those risks that are scored as 'minor' but appear in multiple service risk registers. As a result, whilst the individual risk score is low, these may need to be included in the CRR due to the impact if the risk materialised for all service areas.

- Once the CRR has been reviewed and updated, the Project Management Office produces a risk dashboard to accompany the update report to Standards and Audit committee on a 6-monthly basis for review.

- The Assistant Chief Executive (Section 151 Officer) provides an update to Standards and Audit Committee on a six-monthly basis to report on the Corporate Risk Register and associated activity.

- Risk registers will be shared with internal audit annually (to inform the annual audit plan) with internal audit recommendations being considered by CLT and SLT and triggering updates to service area risk registers where appropriate.

Risk management is an integral part of corporate governance, and in particular, closely linked with corporate performance management. As such, the Council's Risk Management Framework will be reviewed in line with Corporate Business Planning cycle (next review: 2025 for 2026).

Risk management needs to be dynamic in order to capture and anticipate new risks and to assess the trade-off between risk and opportunity. It is an ongoing cycle, that used properly, will help to ensure that effective decisions are made, based on a sound understanding of the risks and opportunities faced.

Risk management can be described in a 5-step process:

Please refer to **Appendix 2: Risk Management Process diagram**

Step 1. Set the Council's objectives and risk appetite.

i. Corporate Business Plan and Service Area Plans

The Corporate Business Plan 2022-2026 and the associated corporate strategies for Economic Development, Empowering Communities, Climate Change, Health and Wellbeing and Organisational Development provides the strategic direction and objectives to be delivered over the period of the plan.

Annual service area plans set out the specific corporate and operational objectives that will be delivered by the teams and individuals in the service area over the following 12-month period.

ii. Risk Appetite

Risk Management is a continuously evolving process, whereby the Council constantly seeks to refine and improve process, in order to support the delivery of its objectives and take a proportionate approach to risk. Identifying its risk appetite enables the Council to take a balanced approach in respect of risk by understanding the risk levels that it may tolerate, and therefore target its scarce resources at the management of risks that cannot be tolerated. Effective risk management supports informed decision-making through the determination of the nature and extent of the principal risk exposure to the Council, and how much risk it is capable of absorbing to achieve its objectives.

It is often not possible to manage all risk to the most desirable level, but the setting of risk appetites and tolerances means that risks can be managed to a tolerable level.

In addition to having an overarching risk appetite statement, the Council has developed statements to describe its attitude to accepting risk in each of its areas of risk categories.

The following risk appetite scale will be use used to assess the level of risk appetite for each area.

Risk appetite	Description
Averse	Avoidance of risk and uncertainty in achievement of key deliverables or initiatives is key objective. Activities undertaken will only be those considered to carry virtually no inherent risk.
Minimalist	Preference for very safe business delivery options that have a low degree of inherent risk with the potential for benefit/return not a key driver. Activities will only be undertaken where they have a low degree of inherent risk.
Cautious	Preference for safe options that have a low degree of inherent risk and only limited potential for benefit/return. Willing to tolerate a degree of risk in selecting which activities to undertake to achieve key deliverables or initiatives, where scope has been identified to achieve significant benefit and/or realise an opportunity. Activities undertaken may carry a high degree of inherent risk that is deemed controllable to a large extent.
Open	Willing to consider all options and choose one most likely to result in successful delivery while providing an acceptable level of benefit. Seek to achieve a balance between a high likelihood of successful delivery and a high degree of benefit and value for money. Activities themselves may potentially carry. or contribute to, a high degree of residual risk.
Eager	Eager to be innovative and to choose options based on maximising opportunities and potential higher benefit even if those activities carry a very high residual risk.

Risk appetite statements will be reflective of commentary within the Corporate Business Plan. In addition, it is anticipated that further detail on the risk appetite for major strategic risk areas such as the holding of investment property, regeneration projects, and capital financing, will be set out in greater detail within specific documents such as the Capital and Investment Strategy.

The overarching Risk Appetite statement and individual risk area appetites will be reviewed annually and feed into the Council's budgetary and policy framework.

An example table of risk appetite levels against a selection of risk categories is set out at Appendix 3: Example Risk Appetite

Step 2. Identify risks.

Common techniques used to identify risks are horizon scanning, brainstorming, workshops and facilitated discussions. Risks are documented in an appropriate risk register.

i. External Threats (horizon scanning)

The Council's horizon scanning process will identify external threats over which it has no direct control. The Council's response to these threats will be an important factor in how it develops and implements the Corporate Business Plan and associated strategies as well as how the Council translates these into service delivery. As such, the Council can draw down any of these threats into the Corporate Risk Register if or when required.

The Service Area Horizon Scanning template incorporates a PESTLE analysis at both the whole organisation and service level to evaluate:

- **Political** - Political factors at local, regional and national level
- **Economic** - Economic factors at local, regional and national level
- **Sociological** - Emerging trends that impact on professional or lifestyle.
- **Technological** - Impact of technological advances or adaptations
- **Legal** - Legal regulations, considerations, relevant National or International case law
- **Environmental** - Environmental factors at local, regional, national or global level
- **Organisation** – organisational factors that could impact on delivery of corporate or service objectives.

Conducting a PESTLE analysis supports identification of risk at the corporate, service, project or contract level that need to be managed in order to successfully deliver objectives. This is a useful exercise for CHoS to complete at least annually as part of business planning.

ii. SWOT Analysis (Strengths, Weaknesses, Opportunities, Threats)

Conducting a SWOT analysis is a useful way to partition factors that could be a risk. Weaknesses and Threats are highlighted as risks and Strengths and Opportunities are identified as opportunities for the service, task or project and as a result risks are determined.

iii. Brainstorming, workshops, facilitated discussions.

Asking the following questions can help identify risks:

- What could happen to stop or delay delivery of objectives?
- What could realistically go wrong?
- What do we need in order to achieve this objective? Do we depend on others to succeed?
- What opportunities might arise?
- What assumptions have been made?
- What have we learnt from delivery of other similar objectives? What were the risks and how have these been addressed? Have they been considered for this objective?

iv. Risk Registers

Risks identified are documented in a Risk Register.

Corporate Risk Register

The Corporate Risk Register (an example is given in Appendix 4) contains key strategic risks which could affect the delivery of the Council's objectives and targets as set out in the Corporate Business Plan and corporate strategies. The owner of this register is CLT. SLT provide significant inputs and support regular and frequent reviews. The risks on this register are often at such a level where only CLT or SLT can influence and mitigate them through political and financial intervention or other means, such as redistributing resources. The risks on the Corporate Risk Register may come from horizon scanning and PESTLE analysis of the wider public sector, local government or market conditions or be unique to the Council in terms of one-off, specific risks. Significant high-scoring risks from service area risk registers will also be escalated to CLT for consideration of inclusion in the Corporate Risk Register.

Service Area Risk Registers

Service Area Plans set-out the aims, objectives, priorities and resources required for delivery of all of the individual services the Council provides. The details of the activities required to deliver each service must be set-out and understood and it is important that specific threats and risks at the operational level are identified and managed. Each CHoS is responsible for maintaining an up-to-date service risk register. These risks are the risks that will be experienced 'on the front line' and will be documented in the related service area risk registers (an example is given in Appendix 4). Significant high-scoring risks from service area risk registers must be escalated to CLT for consideration of inclusion in the corporate risk register.

Project Risk Registers

Every project has a distinct set of objectives and work packages to deliver the required outcomes, and the risks that might impact on these will need to be managed to support delivery on time, budget and quality. Risks should be identified in the business case for the project (Initiation stage) and managed throughout the lifecycle of project. Once the project is authorised, risks should be managed in the project risk register (an example is given in Appendix 4) in accordance with the Project Management toolkit and methodology. Risks should be regularly reviewed at Project Team and Project Board meetings and overall risk status reported as part of the monthly Project Management Office reporting process. Significant high-scoring risks from project risk registers should be escalated to the CHoS to be determined whether it should also be included on the service area risk register.

Contract Risk Registers

Contract Owners and Managers are required to identify risks associated with third party service works or goods delivery and maintain contract risk registers for key Council contracts where the risk of contract failure would result in a significant issue for the Council. These contracts could be categorised as those that deliver a key service to residents, that provide a significant income stream, that are integral to core Council operations or those that would result in major reputational damage in the event of failure. The significance of each contract will vary a great deal, so in these instances, Contract Managers should contact the Corporate Procurement team to discuss the risk management approach that should be applied. Areas to consider will be governance, reporting and monitoring arrangements. The contract management framework covers contract risk in more detail.
Significant high-scoring risks from contract risk registers should be escalated to the CHoS to be determined whether it should also be included on the service area risk register.

Step 3. Evaluate risks

Once risks have been identified, the risks need to be categorised, scored, and rated. The Risk Register template supports this through the use of drop-down selections and calculated cells.

i. Risk Categories

Identified risks are categorised into high-level risk categories (example risk categories below are taken from the Government's Orange Book: Management of Risk – Principles and Concepts[1]):

Strategy risks – Risks arising from identifying and pursuing a strategy, which is poorly defined, is based on flawed or inaccurate data or fails to support the delivery of commitments, plans or objectives due to a changing macro-environment (e.g. political, economic, social, technological, environment and legislative change).

Governance risks – Risks arising from unclear plans, priorities, authorities and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance.

Operations risks – Risks arising from inadequate, poorly designed or ineffective/ inefficient internal processes resulting in fraud, error, impaired customer service (quality and/or quantity of service), non-compliance and/or poor value for money.

Legal risks – Risks arising from a defective transaction, a claim being made (including a defence to a claim or a counterclaim) or some other legal event occurring that results in a liability or other loss, or a failure to take appropriate measures to meet legal or regulatory requirements or to protect assets (for example, intellectual property).

Property risks – Risks arising from property deficiencies or poorly designed or ineffective/ inefficient safety management resulting in non-compliance and/or harm and suffering to employees, contractors, service users or the public.

Financial risks – Risks arising from not managing finances in accordance with requirements and financial constraints resulting in poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting.

Commercial risks – Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, and/or failure to meet business requirements/objectives. Includes procurement risks.

People risks – Risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviours, the unavailability of sufficient capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance.

[1] Annex 4: Example Risk Categories, The Orange Book

Technology risks – Risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience.

Information risks – Risks arising from a failure to produce robust, suitable and appropriate data/information and to exploit data/information to its full potential.

Security risks – Risks arising from a failure to prevent unauthorised and/or inappropriate access to the estate and information, including cyber security and non-compliance with General Data Protection Regulation requirements.

Project/Programme risks – Risks that change programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits to time, cost and quality.

Reputational risks – Risks arising from adverse events, including ethical violations, a lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, leading to damages to reputation and or destruction of trust and relations.

Failure to manage risks in any of these categories may lead to financial, reputational, legal, regulatory, safety, security, environmental, employee, customer and operational consequences.

Most risks will have impacts that span multiple risk categories and therefore risks should be categorised according to the biggest impact on the Council should the risk materialise. High-level risk categories are useful to understand the general nature of a risk and to help ensure the right officers are monitoring and dealing with it.

Risk categories will be used for high-level reporting purposes when the risk dashboard is produced.

Step 3. Scoring Risk

A Risk Score is a calculated number that aims to assess and quantify a level of risk associated with a system, process or activity.

Risks are scored by multiplying their potential severity of impact by the likelihood of their occurrence.

The risk score is calculated pre- and post- mitigation.

Risk score = Impact x Likelihood

i. Impact Scales

If a risk were to materialise, the impact needs to be considered on a variety of levels including impact on strategic and service deliverables, budgets and compliance with relevant law or regulations.

Impact		Considerations			
Score	**Severity of Impact**	**Strategic**	**Delivery**	**Finance**	**Compliance**
5	Critical issue and considerable impact	Failure to deliver council priorities or major project. Council receives nationally adverse publicity perceived as failing in a significant area of responsibility	Failure to deliver a service/project. 50-95% schedule overrun on project	Significant financial loss or overspend £250,000 plus leading to the section 151 Officer having to issues a statutory report. 50-95% project overspend	Breach of law/ regulations leading to significant sanctions Litigation almost certain with minimal defence
4	Serious problem with significant impact	Significant impact on delivery of Council priorities or major priorities Public confidence in council undermined.	Unsatisfactory service performance/service disruption for 5+ days 25%-50% schedule overrun on projects	Financial loss or overspend greater than £100,000-£250,000. 25%-50% project overspend	Breach of law/regulations leading to some sanction Litigation almost certain with some defence
3	Noticeable effect	Possible impact on the delivery of council priorities Significant adverse local publicity	Reduction in service performance / service disruption for 1-2 days	Financial loss or overspend between £50,000-£100,000	Breach of law/regulation or responsibility or internal standard Litigation possible
2	Only a small effect	Minor adverse local publicity Minor impact on staff morale/public attitudes	Poor service / service disruption up to one day 10%-25% project schedule overrun	Financial loss or overspend between £5,000 - £50,000. 10%-25%project overspend	Breach of internal procedure or policy Complaints likely
1	Negligible impact	No significant impact on the delivery of Council priorities Unlikely to cause adverse publicity	No significant difficulty providing a service or delivery of a project. Less than 10% schedule overrun on projects	Financial loss or overspend under £5k	Minor breach of policy or internal procedure Complaints unlikely

ii. Likelihood Scale

The probability that a risk materialises and becomes an issue is determined by the likelihood scale.

Score	Likelihood of Occurrence	Probability	Description
5	Certain to Happen	90%+	Without action, issue is highly likely to occur. No internal controls / mitigating actions in place. The Council is experiencing problems in this area or expects to within the next 12 months.
4	Probably will Happen	60%-90%	Strong possibility. Poor or ineffective internal controls / mitigating actions in place, or existing controls are generally ignored. The Council has experienced problems in this area within the last 12 months.
3	Possibly will Happen	40%-60%	Might occur. Some internal controls / mitigating actions in place, but in need of review / improvement. Existing controls generally work but there have been occasions when they have failed, and problems have arisen. The Council has in the past experienced problems in this area but not in the last 12 months.
2	Unlikely to Happen	10%-40%	Not expected. Effective internal controls / mitigating actions in place. Previous experience discounts this risk as being likely to occur, but other organisations have experienced problems in this area.
1	Highly unlikely to happen	0%-10%	Very unlikely to occur. Substantive, effective, tested and verifiable internal controls / mitigating actions in place. Previous experience at this and other similar organisations makes this outcome highly unlikely to occur

Step 4. Take action to manage risks.

i. Runnymede Borough Council Risk Matrix

When assessing a risk for the first time (including project and contract risks), the pre-mitigation risk score is calculated assuming that the risk is accepted without any controls or mitigation actioned (pre-mitigation). The risk is also scored post-mitigation to calculate a score for the remaining substantive risk assuming the agreed risk action plan is implemented.

Risk score is calculated by assigning values for the identified likelihood of occurrence (A) and the severity of the impact (B). Multiplying ‘A’ and ‘B’ calculates the risk rating score, which gives an indication of significance and priority as seen in the risk matrix below.

The thick black line is the “line of tolerance”. Those risks that are plotted above the line (risk score 10-25) are “out of tolerance” and will be referred to CLT for further oversight and support and consideration for inclusion on the Corporate Risk Register.

LIKELIHOOD (A)	**Certain** 5	5	10	15	20	25	Likelihood of Occurrence (A)	Severity of Impact (B)
	Probable 4	4	8	12	16	20	1- Highly unlikely to happen	1- Negligible impact
	Possible 3	3	6	9	12	15	2- Unlikely to happen	2- Only a small effect
	Unlikely 2	2	4	6	8	10	3- Possibly will happen	3- Noticeable effect
	Highly unlikely 1	1	2	3	4	5	4- Probably will happen	4- Serious problem with significant impact
		Negligible 1	**Small** 2	**Noticeable** 3	**Serious + Significant** 4	Critical + Considerable 5	5- Certain to happen	5- Critical issue and considerable impact
	IMPACT (B)							

ii. Risk Response

Once risk score has been calculated, each risk response should be categorised. There are seven key Risk Response categories to mitigate and manage risk:

Avoid: take action so the threat no longer has impact or can no longer happen
Prevention: terminate the risk
Reduction: treat the risk to reduce the probability of the risk or reduce the impact if the risk were to occur
Transference: pass the risk to a third party e.g., insurance
Acceptance: accept and tolerate the risk
Contingency: action plan implemented to reduce the impact of the risk
Share: share the risk and potential opportunity

iii. Risk Rating Guidance Table

Risk Rating		Guidance to Risk Owners
15-25	Most Risks at this level sit above the tolerance of the Council and are of such magnitude that they form the Council's biggest risks. The Council is not willing to take risks at this level and action should be taken immediately to treat, transfer or terminate the risk.	Identify the actions and controls necessary to manage the risk down to an acceptable level. Report the risk to the Corporate Head of Service to escalate to CLT. Risk to be added to the Corporate Risk Register. If necessary, steps will be taken to collectively review the risk and identify any other possible mitigation (such as additional controls)
	Some of these risks are within the upper limit of risk tolerance. While these risks can be tolerated, controls should be identified to bring the risk down to a more manageable level where possible. Alternatively, consideration can be given to transferring or terminating the risk.	Identify controls to treat the risk impact/ likelihood and seek to bring the risk down to a more acceptable level. Escalate to CLT. Risk to be considered for inclusion on the CRR.
9-12	These risks sit on the border of the Council's risk threshold and so while they don't pose an immediate threat, they are still risks that should remain under review. If the impact or likelihood increase, then risk owners should seek to manage the increase. Risk with a score above 10 should be escalated to CLT and may be included in the CRR.	Keep these risks on the radar and update as and when changes are made, or if controls are implemented. Movement in risks should be monitored, for instance featuring as part of a standing management meeting agenda
1-8	These are low level risks that could impede or hinder achievement of objectives. Due to the relatively low level, it is unlikely that additional controls will be identified to respond to the risk.	Keep these risks on your register and formally review at least once a year to make sure that the impact and likelihood continues to pose a low level.
	Minor level risk with little consequence but not to be overlooked completely. They are enough of a risk to have been assessed through the process but unlikely to prevent the achievement of objectives.	No actions required but keep the risk on your risk register and review at least annually as part of the service planning process

Step 5. Monitor and report on risk.

i. Communicating Risk

All staff need the knowledge and information necessary to enable them to identify and manage risk effectively. Risks identified must be documented in the appropriate level of risk register.

Corporate Heads of Service are responsible for promoting risk assessment and management with their staff individually, at team meetings and at the outset of projects. The Council's Staff Home intranet will include risk management documentation to support staff manage risk in their work.

The opposite point of view to 'risk' is 'opportunity'. All staff should be aware that in the same way that 'risk' is managed out of the Council's programmes and projects, 'opportunities' should be managed to ensure that they are realised.

ii. Escalating high scoring risk

As a result of identification and evaluation of risks, each risk register will consist of risks that score between 1-25. As per the Risk Guidance Table above, those risks that are plotted above the tolerance line (risk score 10-25) are "out of tolerance" and will be referred to CLT for further oversight and support and consideration for inclusion on the Corporate Risk Register. Risks with scoring between 15-25 are classified as "significant" risks. It is the responsibility of the Corporate Head of Service to escalate these risks to CLT. The Project Management Office (PMO) will support this process to compile risks that need to be reviewed by CLT for incorporation on the corporate risk register.

See **Appendix 1: Risk Escalation Process Diagram**

iii. Reporting risk

The PMO will develop a dashboard as part of the corporate reporting system to communicate the risk portfolio to Standards and Audit committee on a 6-month basis to keep elected members abreast of the highest priority risks identified and the mitigation in place.

Mock-up of a Risk Dashboard – actual content and format to be agreed

The Assistant Chief Executive provides an update to Standards and Audit Committee on a six-monthly basis to report on the Corporate Risk Register and associated activity.

Risk registers will be shared with internal audit annually (to inform the annual audit plan) with internal audit recommendations being considered by CLT and SLT and triggering updates to service area risk registers where appropriate.

6. Roles & Responsibilities

A roles and responsibility matrix has been developed to illustrate the roles and responsibilities of all actors and stakeholders in risk management. See Appendix 5: Roles and responsibilities matrix (RACI).

All staff and stakeholders involved in delivery of the Corporate Business Plan, Service Area Plans and business as usual activities have a responsibility to assess and manage risks and identify and apply learning from risks.

6.1. Elected Members

Members have a responsibility to understand the strategic risks that the Council faces and will be made aware of how these risks are being managed through reports to the Standards and Audit Committee.

- All members will have the responsibility to consider the risks associated with the decisions they make and will be informed of these risks in the Committee reports provided.
- Members should not seek to avoid or delegate overall responsibility regarding risk.
- Gain assurance over the effectiveness of the Council's risk management processes (through internal audit, dashboard updates and reports to Standards & Audit Committee)
- Ensure the decision-making Committees act within the agreed risk appetite and tolerance of the Council.
- To consider the effectiveness of the authority's risk management arrangements, the control environment and associated anti-fraud and anti-corruption arrangements.
- Seek assurance that action is being taken on risk-related issues identified by auditors and inspectors.

6.2. Standards & Audit

The Standards and Audit Committee consists of ten Members. Meetings take place five times a year to discuss:

- Ethical standards and issues.
- Code of conduct for Councillors.
- Corporate systems and controls.
- Internal audit activity.
- Risk management policy and strategy.

In relation to risk management, the Committee has oversight of the Council's risk analysis and risk assessments, risk response, and risk monitoring including:

- The establishment of risk management across the organisation, including partnerships.
- Approval of the Council's risk appetite and tolerance.
- Being appraised of the most significant risks.
- Determining whether management's response to risk and changes in risk are appropriate.

6.3. Internal Audit

Internal audit is an independent, objective assurance and consulting activity designed to add value and improve the Council's operations. It helps the Council accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, controls, and governance processes.

- Undertakes an assessment of the Council's risk management and internal control mechanisms as part of the review of corporate governance arrangements.
- Audit reports are provided to Standards & Audit Committee to consider the adequacy of the existing risk management system and recommendations for continuous improvement.

  This role is fulfilled by a third-party service provider.

6.4. Corporate Leadership Team (CLT)

CLT ensure that effective systems for Risk Management and internal controls are in place to support effective and robust corporate governance of the Council.

- Take a leading role in identifying and managing the risks and opportunities to the Council and to set the example and standards for all staff.
- Set the Council's risk appetite.
- Ensure that this framework is communicated, understood and implemented by all Members, managers and staff, and fully embedded in the Council's corporate business planning and monitoring processes.
- Identify, analyse and monitor high-level corporate and cross-cutting risks on a regular basis.
- Actively support and guide the management of highest priority risks and take action to mitigate impact/likelihood.
- Report to Members on the management of corporate and other significant risks and the overall effectiveness of risk management controls.
- Ensure that sufficient resources are identified and provided to enable the development/implementation of risk management.
- Provide overview and challenge over the corporate level risks facing the Council, how these are affected by change and how they are being managed.
- Review and guide on the risk implications of key decisions as part of the Council's governance process
- Ensure and monitor compliance with risk management practices.
- Own the Corporate Risk Register and review on a regular and frequent basis including a quarterly review with SLT.
- To ensure CHoS appropriately maintain, review and update service area risk registers and integrate them in service area plans.

6.5. Assistant Chief Executive (Section 151 Officer)

The CIPFA risk statement relating to the role of the Section 151 Officer states they should ensure that public money is always safeguarded and used appropriately, economically, efficiently, and effectively.

The risk-related activities of the Section 151 Officer include:

- Ensuring that immediate and longer-term implications, opportunities and risks are fully considered, and any decisions are in alignment with the overall financial strategy.

- As a member of CLT, contributes to the effective corporate management of the organisation, including strategy implementation, advising on cross organisational issues, ensuring integrated business and resource planning, risk management and performance management.
- Supports collective ownership of strategy, risks and delivery.
- Supports the effective governance of the organisation through development of corporate governance arrangements, risk management and reporting framework.
- Address the organisation’s arrangements for financial and internal control and for managing risk in Annual Governance Reports.
- Ensure compliance to the policy across the Council including coordinating and reviewing all Service Plan risks on an annual basis.
- To act as a forum for the sharing of best practice

6.6. Senior Leadership Team (SLT) (Corporate Heads of Service)

Each Corporate Head of Service is individually responsible for monitoring the status of the risk registers and action plans for their respective areas of responsibility. SLT are responsible for embedding risk management into the business/service planning of all areas for which they are responsible.

- Ensure that risk management is part of all major projects, partnerships and change management initiatives.
- Be actively involved in the identification and assessment of risks to ensure that their respective areas of responsibility are sufficiently reflected and updated on the appropriate risk register.
- Assign a Risk Owner to each risk, ensuring that any agreed risk action plan is implemented and reviewed, and risks are treated effectively.
- Escalate high-scoring significant risks to CLT for consideration on the Corporate Risk register.
- Ensure that reports of a strategic nature written for Members include a risk assessment of the options presented for a decision.
- Report as required to the quarterly review meeting with SLT on the progress being undertaken to manage the high priority risks within their areas of responsibility.
- To ensure that appropriate risk management training and awareness is provided to relevant Members and staff.
- Respond to risks in accordance with the Council’s risk appetite.
- Monitoring their teams’ risks regularly and at least quarterly.
- Encouraging staff to be open and honest in identifying risk or potential opportunities
- To ensure that all projects have up to date risks and issues logs and key risks are highlighted at the project initiation stage and on an ongoing basis in project status reports.

6.7. Risk Owners

- Once a risk has been identified, a risk owner will be assigned by the CHoS (service, project or contract risk) or CLT (corporate risk). The Risk Owner is responsible for monitoring the risk and ensuring identified actions are undertaken in response. As a result, this role will provide input into regular and frequent risk review for the risks that have been assigned to them.
- Risk ownership is not the same as actually undertaking or being responsible for carrying out actions in response. Rather the role is aimed at ensuring necessary actions take place, otherwise there is a chance management actions may not be completed.
- The best risk owner will usually be someone closely involved in delivering the area of the business where the risk arises.

6.8. Committee Report Authors

- Any proposed new initiative or activity or change being reported to a committee should include a summary of the risk implications to the service area and Council as a whole, as part of the cover report and full business case.

6.9. All Staff

- Demonstrate an awareness of risk and risk management relevant to their role.
- Identify risks within their everyday work processes and working environment and escalate them as appropriate.
- Participate, where appropriate, in ongoing risk management within their teams and areas of responsibility, as part of regular day-to-day activities.
- Actively manage risks and risk actions, where appropriate.
- All staff have responsibility for council risks and must understand their role in the Council's risk management arrangements.
- Complete relevant risk management training on a regular basis

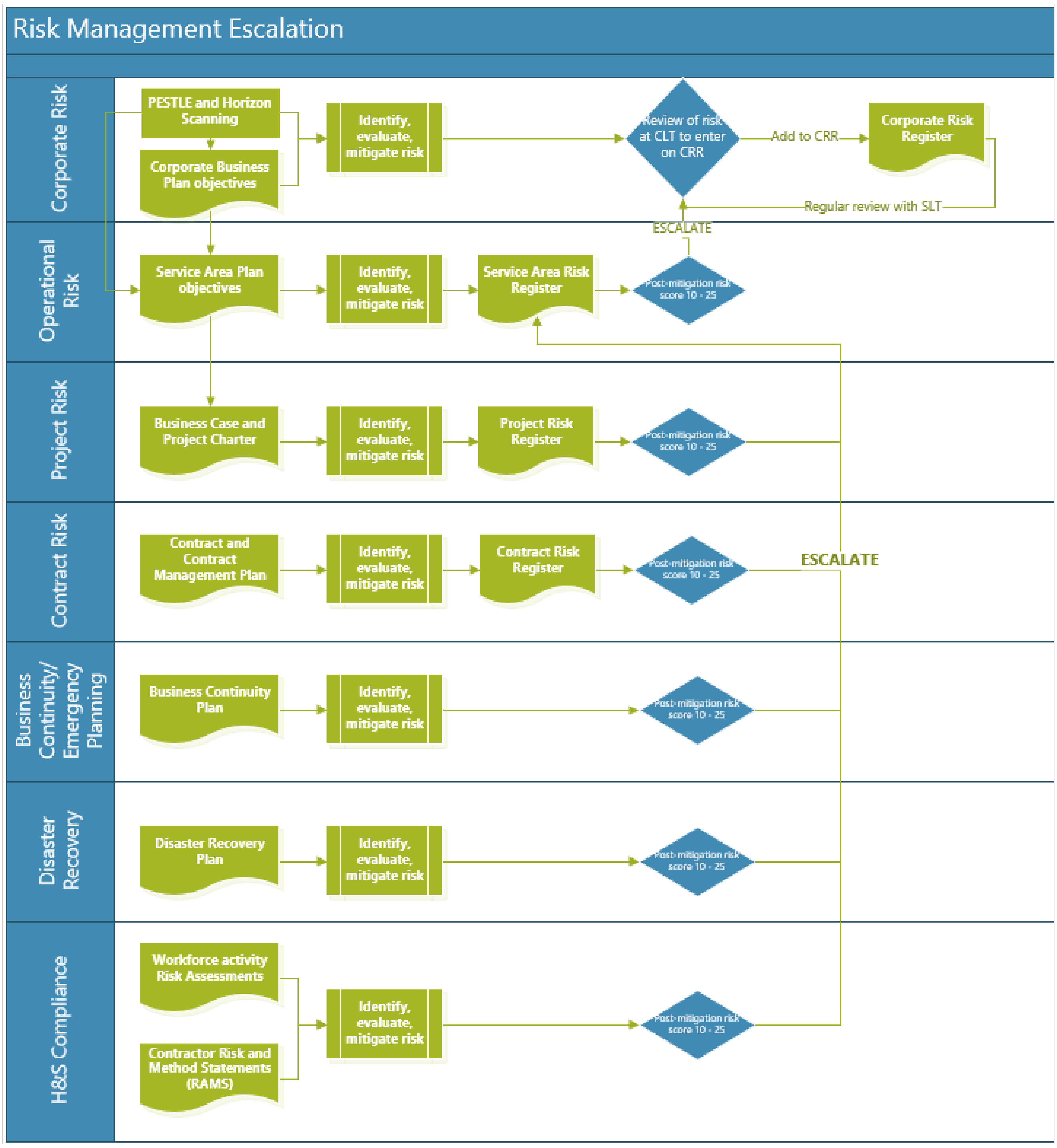
7. Risk Management Training

It is important that elected members and staff develop their knowledge and understanding of risk management.

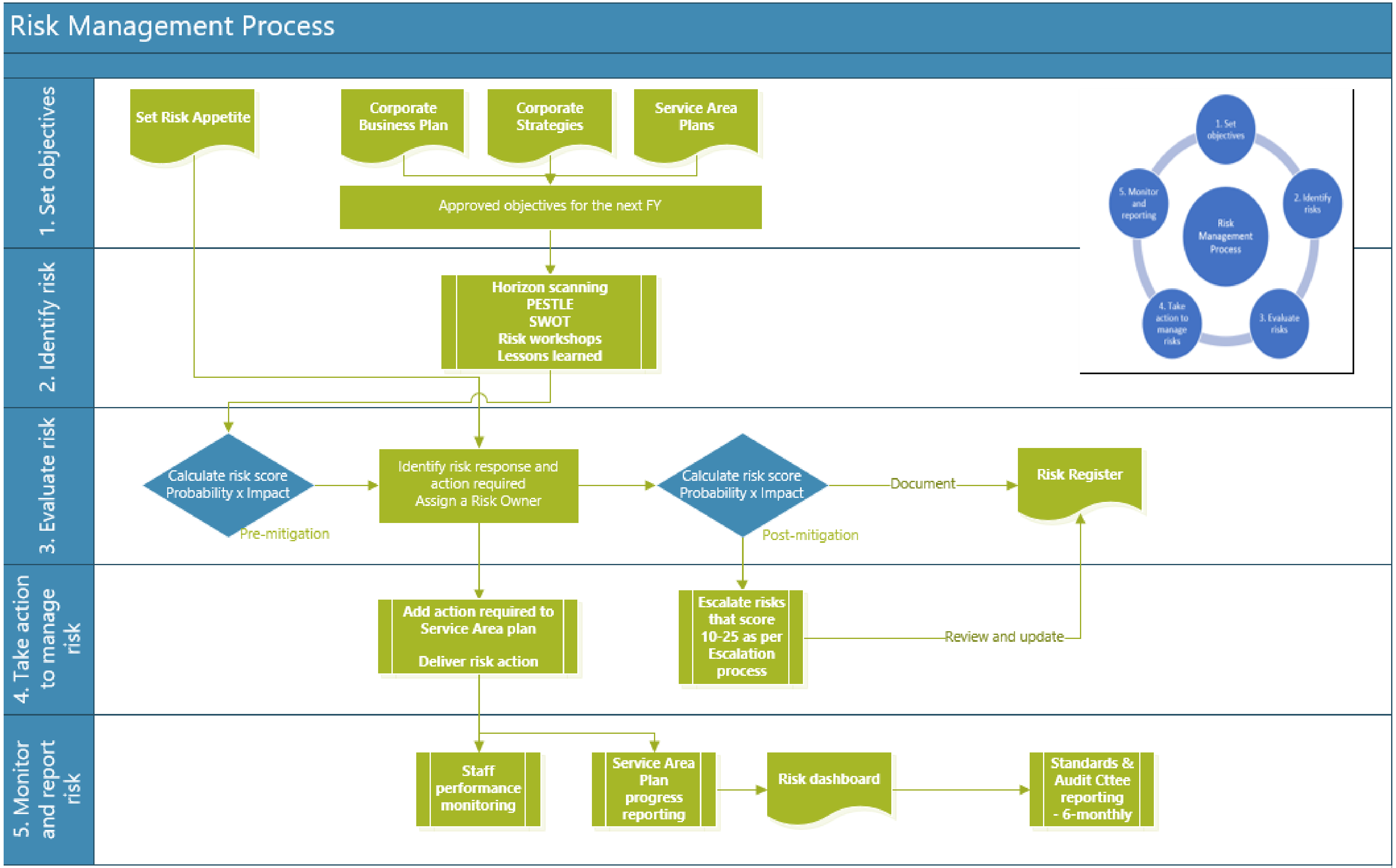
The HR and Organisational Development service area will annually set out as part of the organisation's training programme a variety of training modules addressing risk management that must be completed. Employee training will be appropriate to their role and responsibilities specifically for Risk Management.

The training programme will contain a mixture of both formal and informal training sessions and will remain adaptable to the changing risks within the organisation. Managers will be responsible for ensuring employees within their Service/Team receive adequate Risk Management training and that records of training are retained.

Appendix 1: Risk Escalation Process Diagram



Appendix 2: Risk Management Process diagram



Appendix 3: Example Risk Appetite[2]

	Risk appetite level description				
	Averse	Minimal	Cautious	Open	Eager
Strategy	Guiding principles or rules in place that limit risk in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 5+ year intervals	Guiding principles or rules in place that minimise risk in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 4-5 year intervals	Guiding principles or rules in place that allow considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 3-4 year intervals	Guiding principles or rules in place that are receptive to considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 2-3 year intervals	Guiding principles or rules in place that welcome considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 1-2 year intervals
Governance	Avoid actions with associated risk. No decisions are taken outside of processes and oversight / monitoring arrangements. Organisational controls minimise risk of fraud with significant levels of resource focused on detection and prevention	Willing to consider low risk actions which support delivery of priorities and objectives. Processes and oversight / monitoring arrangements enable limited risk taking. Organisational controls maximise fraud prevention detection and deterrence through robust controls and sanctions	Willing to consider actions where benefits outweigh risks. Processes, and oversight / monitoring arrangements enable cautious risk taking. Controls enable fraud prevention, detection and deterrence by maintaining appropriate controls and sanctions.	Receptive to taking difficult decisions when benefits outweigh risks. Processes, and oversight / monitoring arrangements enable considered risk taking. Levels of fraud controls are varied to reflect scale of risks with costs.	Ready to take difficult decisions when benefits outweigh risks. Processes, and oversight / monitoring arrangements support informed risk taking. Levels of fraud controls are varied to reflect scale of risk with costs.
Operations	Defensive approach to operational delivery - aim to maintain/protect, rather than create or innovate. Priority for close management controls and oversight with limited devolved authority.	Innovations largely avoided unless essential. Decision making authority held by senior management.	Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior management. Management through leading indicators.	Innovation supported, with clear demonstration of benefit / improvement in management control. Responsibility for non critical decisions may be devolved.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust / lagging indicators rather than close control.
Legal	Play safe and avoid anything which could be challenged, even unsuccessfully.	Want to be very sure we would win any challenge.	Want to be reasonably sure we would win any challenge.	Challenge will be problematic we are likely to win, and the gain will outweigh the adverse impact.	Chances of losing are high but exceptional benefits could be realised
Property	Obligation to comply with strict policies for purchase, rental, disposal, construction, and refurbishment that ensures producing good value for money.	Recommendation to follow strict policies for purchase, rental, disposal, construction, and refurbishment that ensures producing good value for money.	Requirement to adopt arrange of agreed solutions for purchase, rental, disposal, construction, and refurbishment that ensures producing good value for money.	Consider benefits of agreed solutions for purchase, rental, disposal, construction, and refurbishment that meeting organisational requirements.	Application of dynamic solutions for purchase, rental, disposal, construction, and refurbishment that ensures meeting organisational requirements.
Financial	Avoidance of any financial impact or loss, is a key objective.	Only prepared to accept the possibility of very limited financial impact if essential to delivery.	Seek safe delivery options with little residual financial loss only if it could yield upside opportunities.	Prepared to invest for benefit and to minimise the possibility of financial loss by managing the risks to tolerable levels.	Prepared to invest for best possible benefit and accept possibility of financial loss (controls must be in place).
Commerical	Zero appetite for untested commercial agreements. Priority for close management controls and oversight with limited devolved authority.	Appetite for risk taking limited to low scale procurement activity. Decision making authority held by senior management.	Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior management. Management through leading indicators.	Innovation supported, with demonstration of benefit / improvement in service delivery. Responsibility for non-critical decisions may be devolved.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust / lagging indicators rather than close control.
People	Priority to maintain close management control & oversight. Limited devolved authority. Limited flexibility in relation to working practices. Development investment in standard practices only	Decision making authority held by senior management. Development investment generally in standard practices.	Seek safe and standard people policy. Decision making authority generally held by senior management.	Prepared to invest in our people to create innovative mix of skills environment. Responsibility for noncritical decisions may be devolved.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust rather than close control.
Technology	General avoidance of systems / technology developments.	Only essential systems / technology developments to protect current operations.	Consideration given to adoption of established / mature systems and technology improvements. Agile principles are considered.	Systems / technology developments considered to enable improved delivery. Agile principles may be followed.	New technologies viewed as a key enabler of operational delivery. Agile principles are embraced.
Data and Information Mgmt	Lock down data & information. Access tightly controlled, high levels of monitoring.	Minimise level of risk due to potential damage from disclosure.	Accept need for operational effectiveness with risk mitigated through careful management limiting distribution.	Accept need for operational effectiveness in distribution and information sharing.	Level of controls minimised with data and information openly shared
Security	No tolerance for security risks causing loss or damage to property, assets, information or people. Stringent measures in place	Risk of loss or damage to property, assets, information or people minimised through stringent security measures	Limited security risks accepted to support business need, with appropriate checks and balances in place	Considered security risk accepted to support business need, with appropriate checks and balances in place	Organisational willing to accept security risk to support business need, with appropriate checks and balances in place
Project/Programme	Defensive approach to transformational activity - aim to maintain/protect, rather than create or innovate. Priority for close management controls and oversight with limited devolved authority. Benefits led plans fully aligned with strategic priorities, functional standards.	Innovations avoided unless essential. Decision making authority held by senior management. Benefits led plans aligned with strategic priorities, functional standards.	Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior management. Plans aligned with strategic priorities, functional standards.	Innovation supported, with demonstration of commensurate improvements in management control. Responsibility for noncritical decisions may be devolved. Plans aligned with functional standards and organisational governance.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust rather than close control. Plans aligned with organisational governance.
Reputational	Zero appetite for any decisions with high chance of repercussion for organisations' reputation.	Appetite for risk taking limited to those events where there is no chance of any significant repercussion for the organisation.	Appetite for risk taking limited to those events where there is little chance of any significant repercussion for the organisation.	Appetite to take decisions with potential to expose organisation to additional scrutiny, but only where appropriate steps are taken to minimise exposure.	Appetite to take decisions which are likely to bring additional Governmental / organisational scrutiny only where potential benefits outweigh risks

[2] Example appetite levels defined by risk categories taken from the Orange Book Risk Appetite Guidance

Appendix 4: Risk register examples

Example Corporate Risk Register

The Corporate Risk Register is maintained by the PMO and is owned by CLT.

The document is restricted to CLT and SLT only.

		Before mitigating measures				After mitigating measures				
Reference	Issue	Likelihood	Impact	Risk score	Mitigation measures and other comments (bullet points reflect the measures, other text is just a comment)	Likelihood	Impact	Risk score	Trend (for next 3 months)	Owner(s)
1	**Income generation strategies fail to achieve targets**	4	5	20	• CLT and Corporate Management Committee regularly review corporate projects. • Thorough project planning. Concerns about additional cost pressures and rent reviews/rent free periods offset by new Property Income Reserve and Property Maintenance Reserve. Big corporates may look to downsize following pandemic which could affect income. They may also request rents based on turnover. There are also leisure centre income concerns. The pandemic has had a significant impact on the commercial rents and car parking income.	4	5	20	↓	CLT
2	**SCC cost reduction measures impact on Borough Council.**	5	4	20	• Two years of funding has been agreed with SCC for services within Community Services. There is a need to look at other ways of making projects sustainable or cease them. There is a risk currently that we are having to pay the C Tax precept over even if it isn't all collected. There is a greater expectation we will take on more services for SCC e.g. parking.	4	4	16	↑	SLT
3	**Current Business Continuity arrangements are not sufficient to deal with a severe disruptive event.**	5	4	20	Preliminary corporate business continuity audit results are positive. Concerns regarding business continuiuty capacity for monitoring community alarms within Safer Runnymede – contingency planning within Digital Services to address the risk. Corporate review of service level business continuity plans recommended for loss of power and loss of ICT (cyber attack) due to increasing risk in these areas. Corporate cyber attack exercise delayed until September to allow Digitial Services to progress the DR elements. Cyber exercise further delayed due to staff availability. • Corporate Heads reviewing business continuity plans for loss of power planning.	5	4	20	→	SLT/MS/CY
4	**Reduction in the number of existing and new PRS opportunities to place households in private rented sector**	5	4	20	• New PRS Offer to be developed with additional resources being directed to this area. • Entering into innovative partnerships with private owners to make more properties available for our nominees at Local Housing Allowance rents. • New member of staff and additional funding obtained Won't improve in the near future due to economic conditions.	4	4	16	→	CLT + MW

Example Service Area Risk Register

Each service area risk register is owned by the relevant CHoS. It may be maintained by an officer within the service area who has been delegated this task. However, the CHoS is ultimately responsible and accountable for the risk register for their service area.

The document is stored in the Business Planning teams area.

Ref	Issue	Consequences	Impact area *Life and limb Reputational Financial Legal Other*	Probability *(Pre-control measures)*	Impact *(Pre-control measures)*	Risk Rating *(Pre-control)*	Control Measure(s)	Probability *(Post control measures)*	Impact *(Post control measures)*	Rating *(Post control)*	Owner
HR1	Housing Revenue Account Income forecast not met.	Potential increase in rent arrears. Increase in homelessness Drain on bad debt provision KPI for rent arrears affected	Financial	4	5	20	Key performance indicators – monitored by Housing Committee Systems and procedures Annual review of Housing Revenue Account Business Plan	3	4	12	CHoH
HR2	Reduction in the number of existing and new PRS opportunities to place households in private rented sector	Increased strain on homelessness provision. Increased pressure on Housing to source alternative options with potential increase in costs	Delivery of services Welfare of residents Financial Reputational	5	4	20	New PRS Offer to be developed with additional resources being directed to this area. Entering into innovative partnerships with private owners to make more properties available for our nominees at Local Housing Allowance rents. New member of staff and additional funding obtained	3	3	9	CHoH
HR3	Failure to comply with regulator's code	Reputational damage to the Council if inspected by the regulator Financial consequences for not being compliant Concern regarding the quality of service being delivered to tenants and leaseholders	Reputational Financial Delivery of services	4	4	16	KPI framework ISO 9001 policy and procedure framework Key strategic documents Housing Committee oversight	2	4	8	CHoH
HR4	Claims for disrepair from tenants against the Housing Service	Tenants living in homes which are in poor condition Financial compensation to tenant paid Reputational damage to the Council	Financial Reputational Delivery of services	5	3	15	Key tenders in place Effective IT systems – audit trail of repair work Programme of tenancy audits and property inspections in place	3	3	9	CHoH

Example Project Risk Register (grade A projects)

Risk Register - *SHBC/RBC Community Services Partnership*

Runnymede

Project Execution Stage

Initial Risk Identification should be a group activity with the Project Team and Risks should be routinely reviewed as an action on Project team agendas

Risk ID	Risk Description	Risk Assessment Enter 1-5; 5 being highest, 1 being lowest		Risk Score P x I See Risk Matrix	Risk Owner Name | Department	Risk Response	Mitigation	Status	Actions	Update
		Probability	Impact							
Risk001	SHBC Executive do not approve the Partnership to go ahead.	2	5	10	Darren Williams, Corporate Head of Community Services	Reduce	Ensure Executive report promotes fully the benefits of progressing with the Partnership.	Closed	N/A	N/A
Risk002	SHBC TUPE Consultation results lead to the expansion of the Partnership not being agreed by SHBC Cabinet.	2	5	10	Darren Williams, Corporate Head of Community Services Fiona Skene Human Resources & Organisational Development	Reduce	Ensure Consultation steps communicated clearly to participants and issues are resolved in a timely fashion.	Closed	TUPE Information exchanged	TUPE to be completed on 01/04/21
Risk003	Income levels from a further integrated partnership with SHBC are not be realised.	2	3	6	Darren Williams, Corporate Head of Community Services	Reduce	Ensure senior RBC management are fully appraised of the progress of the Partnership merger so contingency plans can made if the income levels are not realised.	On-going	N/A	N/A
Risk004	ICT Equipment not in place for 01/04/21	2	4	8	Darren Williams, Community Services Stephen Bowen, Digital Transformation Manager	Reduce	Work with SHBC and RBC ICT to ensure equipment is in place prior to 01/04/21.	Closed	Monitor	Majority of equipment in place, phones in place and RBC ICT will attend Surrey Heath House on 01/04/21 to ensure smooth transition.

Appendix 5: Roles and responsibilities matrix (RACI)

RACI Matrix for Risk Management Levels at RBC

Key:

D	Driver	Assists those who are responsible for a task.
R	Responsible	Assigned to complete the task or deliverable.
A	Accountable	Has final decision-making authority and accountability for completion. Only 1 per task.
S	Support	Provides support during activity/task.
C	Consult	An adviser, stakeholder, or subject matter expert who is consulted before a decision or action.
I	Inform	Must be informed after a decision or action.

Level	Activity (Role →)	Members	Standards & Audit Cttee	Internal Audit	Corporate Leadership Team (CLT)	Assistant Chief Executive (Section 151 Officer)	Strategic Leadership Team (SLT) (Corporate Heads of Service)	Risk Owner	PMO	Procurement	Committee Report Authors	Contract Owners	Contract Managers	Project Sponsors	Project Managers	All Staff
Corporate Risk Management	Set the Council's risk tolerance and appetite	C	C	D	A	R	I		I							I
	Review the Corporate Risk Register on a regular basis		I		A		R		S							
	Ensure all Corporate Heads of Service are aware of corporate risks, and facilitate a forum to collectively discuss the risks, and develop and plan mitigation				A	R	I		S							
	Provide a checkpoint to ensure that similar risks from across the organisation are being consistently scored				A		I		R							
	Provide a checkpoint to identify those risks that are scored as 'minor' but appear in multiple service risk registers				A		I		R							
	If an individual risk score is low, these may need to be included in the CRR due to the impact if the risk materialised for all service areas.				A		I		R							
	Once the Corporate Risk Register has been reviewed and updated, a risk dashboard is produced to accompany the update report to Standards and Audit committee on a six-monthly basis for review.	I			A		I		R							
	Provides updates to Standards and Audit Committee on a six-monthly basis to report on the Corporate Risk Register and associated activity		I		I	A			S							
	Risk registers will be shared with internal audit annually (to inform the annual audit plan)			I		A			S							
	Internal audit recommendations are to be considered and may trigger updates to service area risk registers		I		I	A	R		S							
	Actively manage risks and risk actions				A		R		S							
Service Level Risk Management	As part of the annual business planning cycle, Service Area Plans and risk registers are developed.	C			A		R		S							
	As part of the drafting of the risk register, risk scores, mitigations and risk owners are to be detailed				A		R	I	S					C	C	
	Identification of risks may lead to necessary action to mitigate the risk and these activities need to be included in the Service Area Plan						A		S							
	Significant risks within these risk registers above the threshold risk score are to be escalated to CLT for consideration of inclusion on the Corporate Risk Register				A		R	I	S							
	On a quarterly basis, service area risk registers are to be reviewed						A	R	I			C	C	C	C	
	Any changes to risks, existing and planned controls, progress against any related risk actions and risk ratings are to be updated on the register by the risk owners						A	R	I							
	Actively manage risks and risk actions						A	R	I			C	C	C	C	
Project Level Risk Management	Risks should be identified in the business case for the project (Initiation stage)								S					A	R	
	Set project risk tolerance						I		S					A		
	Once the project is authorised, risks should be managed in the project risk register in accordance with the Project Management toolkit and methodology.								S					A	R	
	Risks should be regularly reviewed at Project Team and Project Board meetings													A	R	
	Overall risk status reported as part of the monthly Project Management Office reporting process.								I					A	R	
	Significant risks within these risk registers above the threshold risk score are to be escalated to SLT/CLT for consideration of inclusion on the Service Area Plan/Corporate risk registers				I		I							A	R	
	Actively manage risks and risk actions													A	R	
Contract Level Risk Management Process	Contact the Corporate Procurement team to discuss the risk management approach that should be applied depending on governance, reporting and monitoring arrangements.									S		A	R			
	Identify risks associated with third party service works or goods delivery and maintain contract risk registers for key Council contracts where the risk of contract failure would result in a significant issue for the Council.						I					A	R			
	Risks to be regularly reviewed						I			I		A	R			
	Significant risks within these risk registers above the threshold risk score are to be escalated to SLT/CLT for consideration of inclusion on the Service Area Plan/Corporate risk registers				I	I	I					A	R			
	Actively manage risks and risk actions											A	R			

For all information contained within this document contact:

Runnymede Borough Council
The Civic Centre
Station Road
Addlestone
Surrey KT15 2AH

Tel 01932 838383

email: amanda.fahey@runnymede.gov.uk

www.runnymede.gov.uk

Further copies of this publication, or copies in large print other formats or languages can be obtained via the above contact details.

Search: Runnymede Borough Council

Runnymede BOROUGH COUNCIL