www.slough.gov.uk
Slough Borough Council

Growing a place of opportunity and ambition

Appendix C

Risk Management Strategy

Incl. Policy, Procedures, and Guidance

2025

Version Control

Date	Version	Author	Description	Approved by	Date
22nd June 2016	1.0	Phil Brown	Update on 2013 to 2015 Strategy		
14th July 2016	2.0	Phil Brown	Update following Risk Management Group		
22nd Oct 2018	3.0	Phil Brown	Update requirement		
1st Nov 2018	3.0	Phil Brown	Risk Management Board	Risk Management Board	
21st Nov 2018	3.0	Phil Brown	To CMT for Approval	CMT	
13th Dec 2018	3.1	Phil Brown	To Audit & Corp governance for approval	Audit & Corporate Governance Committee	
12th June 2019	4	Phil Brown	Terms of Reference Updated	Audit & Corporate Governance Committee	
2020	5	Phil Brown	Addition of Risk appetite		
March 2022	6	Clare Priest	Annual Review	Risk and Audit Board, CLT , Audit and Corporate Governance Cttee Cabinet	March 2022 April 2022 April 2022 May 2022
Oct 23	7.0	Phillip Watkins	Annual Review		
March 2025	8.0	William Green	Full Revision of Risk Strategy	RMB DLT CLT ACGC Cabinet	May 2025 Aug 2025 Sept 2025 Nov 2025 Nov 2025

Next review date:	**November 2027**

Table of Contents

EXECUTIVE SUMMARY

This Risk Management Strategy establishes a comprehensive approach to identifying, assessing, mitigating, and monitoring risks across Slough Borough Council ("SBC"). The strategy consists of three interconnected components: a Policy that outlines our risk management principles and responsibilities; a Framework that defines our systematic approach to risk management processes; and practical Guidance for implementation.

Our risk management approach is designed to protect organisational value while supporting strategic objectives and operational resilience. It emphasises proactive risk identification, consistent assessment methodologies, and appropriate response mechanisms. The strategy establishes clear accountability at all levels, from the Corporate Leadership Team ("CLT") to individual employees, ensuring risk management becomes embedded in our organisational culture and decision-making processes.

This document serves as the cornerstone for developing a mature risk management capability that enhances our ability to respond to uncertainties, capitalise on opportunities, and maintain compliance with relevant regulations. Implementation will follow a phased approach with regular reviews to ensure continuous improvement of our risk management practices.

The Risk Management Strategy will be maintained by the Risk Management Board and reviewed annually. Updates will be made to reflect any changes in the Council's risk profile, regulatory environment, or industry best practices. Any amendments will be approved by the CLT and communicated to all stakeholders.

1.0 RISK MANAGEMENT POLICY

1.01 Purpose and Objectives

The CLT has overarching responsibility for ensuring the effectiveness of the risk management and internal control systems, supported by the Audit and Corporate Governance Committee, which maintains oversight over the principal risk landscape and how the Council is responding.

The risk management policy (the "policy") sets out the principles for effectively managing the risks in a standard and consistent approach for the identification, assessment, response and monitoring of risk; and, to ensure the Council takes informed and controlled risk-based decisions taking into account our risk appetite.

1.02 Scope and Key principles (describing our approach)

This policy sets out the risk management approach to managing risks (threats and opportunities) to effectively deliver our business plans and purpose.

It applies to all SBC employees, contractors and business partners working with SBC.

The aim of this policy is to establish and promote the use of risk management principles and practices to support delivery of business objectives and attain high standards of corporate governance. To achieve this, we will:

- Establish a risk management framework which delivers a standardised and consistent end-to-end risk management process across all directorates to embed risk management into our culture, processes and practices, and decision making based on the globally recognised risk management framework ISO 31000:2018
- Assign an 'accountable senior leader' to deliver and maintain the risk management framework
- Integrate the management of risk into our management planning activities to ensure the achievement of its strategic objectives
- Apply and incorporate the risk management framework into our operational activities
- Undertake activities within approved risk appetite levels set by the CLT
- Comply with the requirements of the risk management framework and look to continually improve the effectiveness of risk management, such that all reasonably foreseeable risks are systematically identified, assessed, analysed, prioritised and considered for appropriate treatment

Where appropriate we will consider the cost of risk when making decisions about risk treatment options evaluating the financial impact of potential risks against the cost of implementing mitigation measures within our local authority context. This includes assessing the potential financial losses from risk events that could affect service delivery, the cost of preventive measures and controls, staff resources required for risk monitoring, and the potential impact on council budgets and public funds. By comparing these costs with the expected benefits of risk reduction, we can make informed decisions that demonstrate value for money whilst ensuring we maintain appropriate risk levels to safeguard council operations.

1.03 Risk Appetite Statement

SBC is committed to ensuring the effective management of risks while achieving its strategic objectives and delivering public services. The Council recognises that risk is an inherent part of decision-making, and a clear understanding of its risk appetite is essential for balancing opportunity with prudent risk-taking.

The Authority's risk appetite reflects its commitment to delivering value for money, safeguarding public trust, and ensuring the sustainability of its services. This statement outlines the Council's approach to managing risk across all areas of its operations, including financial, operational, regulatory, reputational, and strategic risks. To apply risk appetite effectively, there are six key steps to follow:

- Identify business objectives and review overall strategy
- Understand baseline risk management maturity
- Define risk appetite, considering current risk management maturity and organisational culture
- Integrate risk appetite into decision-making through performance targets
- Specify monitoring, reporting and review processes
- Implement continuous improvement processes, including regular review of risk appetite, cultural maturity and changes in strategy

1.04 Responsibilities

When working for SBC, employees, contractors and business partners must:

- Understand and comply with this policy and take responsibility for their actions, and speak up if something doesn’t look right
- Embed the Risk Management framework, including supporting guidelines and tools, within the directorate business as usual processes
- Align and integrate any local risk management processes with the overall SBC risk management framework
- Prepare, facilitate and support the risk management reporting process for their directorate and the risk management team’s reporting requirements

(including obtaining review and sign-off by the directorate's executive leader pre-submission)
- Escalate and report any significant risks that are outside of their scope of influence and delegation, including emerging risks through the chain of management, to an accountable or responsible colleague and/or to the risk management team

The Cabinet role is to set the risk appetite and influence the culture of Risk Management within the Council, this includes:
- Ensuring risks are considered as part of every Cabinet report decision.
- To review the content of the Corporate Risk Report at least annually, ensuring procedures are in place to monitor the management of the corporate risks to reduce the likelihood of unwelcome surprises.
- Periodically review the Council's approach to Risk Management and approve changes or improvements to key elements of its processes and procedures.

The Corporate Leadership Team ("CLT") and Directorate Leadership Teams ("DLT") will:
- Promote, develop and support risk management and risk management culture
- Identify, assess and evaluate corporate, material and emerging risks and ensure that material risks are managed and mitigated effectively

The Risk Management Board will:
- Be responsible for the Councils' risk management programme and monitoring the corporate risks.
- setting risk management guidelines. contributing to the setting of policies and processes for monitoring and managing our risks.
- A copy of the Corporate Risk Report will be submitted to the CLT on a quarterly basis and thereafter to the Audit & Corporate Governance Committee.

The Risk Management team will:
Develop and manage the risk management framework, including:
- clearly defining and documenting accountabilities of all stakeholders
- providing the appropriate guidance, tools and training to promote and embed risk management practices across the business
- Coordinate, prepare and facilitate the risk reporting process
- Oversee risk management activities and act as advisor to risk owners and the directorates

Internal Audit will provide assurance on the management of risk including, but not limited to:

- The implementation of a risk-based audit plan
- Reviewing the adequacy of risk management processes across the council

1.05 Performance Management

The review, monitoring, approval and reporting of compliance with the principles of this policy are achieved through the following:

- CLT members, with the support of the Directorate DLT's, preparing and submitting quarterly corporate risk dashboards and directorate risk registers to the risk management team
- The risk management team providing technical risk management support across the business and continual improvement of the risk management framework
- The risk management team providing assurance over our corporate risks on a quarterly basis to the CLT and the Audit and Corporate Governance Committee
- The risk management team reporting on the effectiveness of this policy and significant non-compliance to the CLT and the Audit and Corporate Governance Committee

1.06 References

Internal:

Risk Management Framework Standard

- Risk Management Board Terms of Reference *(Link)*
- Audit and Corporate Governance Committee Terms of Reference *(Link)*

External:

- ISO 31000: 2018 international risk management standard

2.0 RISK MANAGEMENT FRAMEWORK

2.01 Executive Summary

SBC is committed to robust standards of corporate governance and follows the requirements of the 'Good Governance in the Public Sector' which sets out a number of main principles of good governance, and the responsibility of the CLT and the Audit & Corporate Governance Committee ("A&CGC"). As part of these commitments, the CLT and A&CGC are responsible for monitoring and reviewing the effectiveness of our risk management programme.

This framework forms a key part of the overarching Risk Management programme, which provides a set of components that lay out the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the business.

The risk management framework is aligned to the International Standard, ISO31000:2018 Risk Management, to establish a uniform and consistent risk management programme which supports compliance with the 'Good Governance in the Public Sector'.

2.02 Objectives

This standard describes the minimum risk management requirements all directorates are required to meet, to demonstrate that they are managing risk effectively.

Detailed guidance, information and risk management support is available from the risk management team.

2.03 Scope and Applicability

Scope

The scope of the framework extends to all reasonably foreseeable risks that we face.

Applicability

Application of this Council framework applies to employees, temporary staff, third parties or contractors, working for or with SBC (collectively referred to as colleagues) when undertaking the activities described.

For SBC employees, breach of this standard may result in disciplinary action, up to and including dismissal. Breach of this framework by any individual who is not a SBC employee may result in other appropriate action being taken in relation to the individual and/or the business which supplies services to SBC, including termination of the relevant contract(s).

2.04 Expectations and Performance Requirements

This framework sets out the minimum expectations and performance requirements to operate a robust risk management programme.

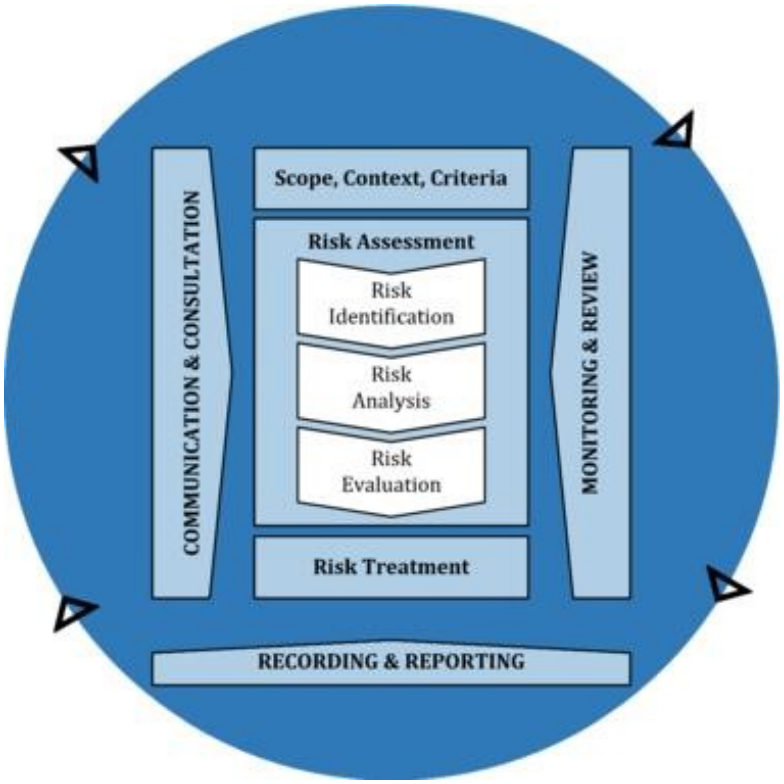
Overview

We are committed to maintaining a straightforward and transparent approach to risk management, that promotes risk awareness, continuous improvement and the management of risk (threats and opportunities) at all levels of the organisation.

Risk Management Process

The risk management process is designed in accordance with the globally recognised risk management framework ISO 31000:2018, as shown below, and must be adopted by all directorates.

Figure 1 – ISO 31000:2018 Enterprise Risk Management Process



The key outputs from this process are the creation of corporate risk dashboards and individual directorate risk registers that support identification of actions and controls to manage risks, and key risk indicators to predict potential risks that can negatively impact the council. All risk scoring must be undertaken using the risk assessment matrix *(Guidance section appendix 4.02, page 34)*.

Guidance on populating the principal risk dashboards and individual directorate risk registers, and the scoring and treatment of risks, can be found in the Risk Management Guidance (page 18).

Establishing the context

By establishing the context, SBC articulates its objectives, defines the internal and external parameters to be considered when managing risk and sets the scope and risk criteria for the risk assessment. The context should include both internal and external parameters relevant for the Council. While many of these parameters are similar to those considered in the design of the risk management framework, when establishing the context for the risk management process, they need to be considered in greater detail and particularly how they relate to the scope of the particular risk management process

Communication and consultation

Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process. Communication and consultation with stakeholders is important as they make judgements about risk based on their perceptions of risk. These perceptions can vary due to differences in values, needs, assumptions, concepts and concerns of stakeholders. As their views can have a significant impact on the decisions made, the stakeholders' perceptions should be identified, recorded, and considered in the decision-making process Communication and consultation should facilitate truthful, relevant, accurate and understandable exchanges of information, considering confidential and personal integrity aspects

Responsibilities

The Risk Management policy sets out the risk management responsibilities for managing risk. In addition, directorates must allocate adequate resources to:

- Establish directorate Risk Champions
- Support and develop managers to manage risk

The minimum responsibilities of these roles must be maintained by the risk management team. The responsibilities of other risk management roles, such as project risk managers etc, are defined by directorate management in the relevant business area. A summary of what all roles in the risk management process are expected to do is provided in *appendix C, page 15*

Any governing body or individual with responsibilities within the Risk Management framework must retain evidence to demonstrate compliance with the Risk Management policy and this framework.

2.05 Risk Management Guidelines

The risk management guidelines (see section 3, page 18) are a reference aid in how to use and apply the risk management process. Where the risk management guidelines are not adopted, management still need to ensure that local processes are compliant with the mandatory requirements of the Risk Management policy and this overall Risk Management strategy.

2.06 Risk Taxonomy

Our risk taxonomy provides a standardised framework to describe our risks across SBC and we have split our risk taxonomy into two levels, strategic and directorate which will provide a comprehensive view of our potential risks.

The four principal risk categories which are applicable are listed below:

- Strategic Risk - Risks related to Organisational goals and strategic decision-making.
- Compliance Risk - Risks related to regulatory requirements and legal obligations.
- Operational Risk - Risks arising from internal processes, systems, and human factors.
- Financial Risk - Risks impacting financial performance and economic stability.

Our current risk taxonomy for our corporate risks (see 2.07 appendix B for a definition of a corporate risk) is as follows:

Corporate Risk	Corporate Risk
CR01: Safeguarding Children and Young People – Child Death	CR08: ICT incident resulting in significant data and/or service
CR02: Failure to meet demands on Adult Social Care	CR09: Failure to achieve financial sustainability and a balanced MTFS
CR03: Failure of Special Educational Needs and Disability (SEND)	CR10: Failure of General Fund Asset Disposal Programme
CR04: Failure to Provide Safe Temporary Accommodation within Budget	CR11: Failure to become a Best Value Council
CR05: Failure to Attract Retain & Engage with Our People	CR12: Failure to deliver Market Sustainability across Council
CR06: Health & Safety We fail to prevent physical injury or mental harm	CR13: We fail to comply with GDPR data protection obligations
CR07: Insufficient Operational Resilience and Crisis Management	CR14: Failure of Council Subsidiary Companies

To ensure that we have a common approach at the directorate level, the following breakdown of possible risks should be used as a starting point to identify risks when completing the directorate/departmental risk registers.

Strategic • Service performance failure • Brand reputation • Strategic partnerships • Significant financial failure • Technological disruption • Fraud	**Digital & Cyber** • Data breaches • Ransomware attacks • System vulnerabilities • Technology integration challenges • Cloud security issues
Operational • Process failures • Equipment malfunction • Human error • Supply chain disruptions • Inefficient workflow • Data management issues	**Environmental & External** • Natural disasters • Pandemics • Political instability • Climate change impacts • Economic recessions
Financial • Credit risk • Market volatility • Investment uncertainties • Liquidity challenges • Budget overruns	**Reputational** • Social media controversies • Ethical misconduct • Customer dissatisfaction • Service issues
Regulatory & Legal • Regulatory changes • Non-compliance penalties • Contract disputes • Intellectual property challenges • Litigation risks • Environmental regulations	**People** • Skill gaps • Leadership succession • Employee turnover • Workplace culture challenges • Training and development limitations

2.07 Appendices

Appendix A: Abbreviations

SBC	Slough Bourgh Council
CLT	Corporate Leadership Team
BAU	Business As Usual
RM	Risk Management
DLG	Directorate Leadership Group
ACGC	Audit and Corporate Governance Committee

Appendix B: Terms & Definitions

Risk Management	Our council-wide approach to risk management that enables us to consider the potential impact of all types of risks on all our processes, activities, stakeholders, assets and services.
Corporate Risk	A risk or combination of risks that can seriously affect our future prospects or reputation. These should include risks that threaten our business model, future performance, solvency or liquidity.

Appendix C: Roles and Responsibilities

Group/Stakeholder	Role Description
Cabinet	• Set the risk appetite and influence the culture of Risk Management within the Council. • Periodically review the Council's approach to Risk Management and approve changes or improvements to key elements of its processes and procedures.
Audit and Corporate Governance Committee	• Review the effectiveness of risk management arrangements. • Provide comment and challenge on risk management activity and progress.
Corporate Leadership Team	• Overall accountability for risk management across the business including ensuring the corporate risk dashboards are live and up to date record of the current corporate risks. • Set the tone for risk management, promote the benefits of effective risk management and lead by example in embedding the risk management framework.

	• Establish a control environment and culture where risk can be effectively assessed and managed. • On a quarterly basis review the corporate risk report.
Risk Management Board	• Monitors and reviews the effectiveness of the risk management programme, including approving the Risk Management policy. • To ensure that there is a clear process in place to allow Corporate Leadership Team, Audit & Corporate Governance Committee and Cabinet to have assurance that risk is being robustly managed within the authority. • Assesses and evaluates the corporate, material and emerging risks that we face, ensuring they are managed effectively. • Ensure any emerging risks identified through governance reporting are escalated in accordance with the Risk Management framework.
Executive Director Corporate Resources	• Overall accountability for the effective delivery of the organisation's risk management function in accordance with industry best practice. • Ensure risk management features as part of the organisations proper administration to protect the authority from financial and reputational risk.
Directorate Leadership Teams	• Accountable for identifying risks to our operations within their directorates and ensure that material risks are managed effectively. • Identify any shared risks (impacting more than one directorate) and manage them through communication, collaboration and/or coordination by the impacted directorates. • Develop, promote and support the risk management culture within their directorates.
Departmental Leads/Heads of Service	• Embed our risk management approach into BAU processes and include risk management as a regular management meeting agenda item to allow consideration of risk exposures and risk informed decision-making. • Embed adequate controls to manage risks related to the department, facilities and assets under their scope of influence and delegation. • Escalate and report any significant risks that are outside of their scope of influence and delegation, including emerging risks through the chain of

	management, to an accountable or responsible colleague and/or to the risk management team.
Risk Champion	• Main link between Risk Management team and their respective directorate. • Improve the Directorate's alignment to SBC RM framework through training and support of directorate staff. • Understand, support, and facilitate the delivery of the RM framework. • Work closely and support action owners. • Provide input, where necessary, to directorate head as part of the sign-off process.
Risk Owners	• Assess risks for the processes under their management. • Implement risk treatment strategies for the risks under their management. • Monitor risks under their management. • Respond to the risks under their management. • Ensure the accuracy and timeliness of information provided for risk reporting.
Risk Treatment Plan Action Owner	• Support risk owners in implementing risk response strategies. • Support risk owners in responding to tolerance breaches. • Support risk owners in providing accurate and timely data for risk reporting.
All employees, temporary staff, third parties or contractors	• Maintain awareness, understanding and compliance with the Risk Management framework as it applies to their role while working for or on our behalf.
Head of Internal Audit	• The implementation of a risk-based audit plan • Reviewing the adequacy of risk management processes across the council.

3.0 RISK MANAGEMENT GUIDANCE

3.01 Purpose

The purpose of this document is to provide guidance for implementing effective Risk Management within our organisation. Adherence to this guidance allows for significant/material risks from across all parts of the Council to be brought together to enable senior leadership to oversee their management, make risk-informed decisions and prioritise treatment strategies.

It aims to establish a standardised approach to identify, assess, and manage risks (threats and opportunities), fostering a risk-aware culture that contributes to the achievement of effectively delivering our business plans and purpose.

3.02 Introduction

Risk management is a systematic and integrated approach to identifying, assessing, and managing risks across all levels of our business.

Our Risk Management team have responsibility for risk management across the council, providing expertise and support to the directorates and reporting risk information to the Risk Management Board, CLT,and the Audit & Corporate Governance Committee

Risk is defined as the uncertainty surrounding events and their outcomes that may have a significant effect on:

- Operational performance
- Achievement of aims and objectives; or
- Meeting expectations of stakeholders

Risk is an inherent feature of all activity and may arise from inaction as well as from undertaking new initiatives. Risks can be conventional threats to an organisation; they can also be positive opportunities. Consideration of risk will encompass an assessment of risk taking – the level of risk the Council is prepared to take to innovate and/or achieve its strategic and business objectives falls within our overall risk appetite.

In an ever-evolving local authority landscape, understanding and proactively addressing risks is essential for sustaining success and creating long-term value. This guidance document supports the embedding of our risk management principles into our organisational culture, ensuring a holistic and consistent approach.
As a Council, effective risk management will enable:

- Increased confidence in achieving desired outcomes and objectives.
- Management of threats to an acceptable level.
- Exploiting opportunities when appropriate.

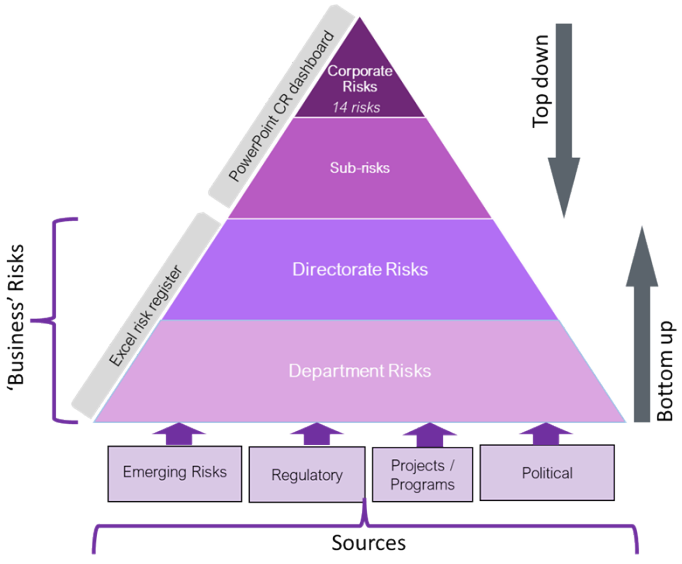
3.03 Risk Structure

The Risk Management Framework utilises the following risk structure:

- Corporate risks are the most material risks (strategic, operational, financial and compliance) to the council that can seriously affect our future prospects or reputation. These should include risks that threaten our business model, future performance, solvency or liquidity.
- Each corporate risk is built up of two or more sub-risks, providing the detailed breakdown of risks within the overarching corporate risk.
- Individual directorate risks are the specific risks identified and managed within a directorate, including material risks as identified by the department line management.
- We currently have 14 corporate risks as at Q1 FY25/26. This number may change over time.
- The risk management process is based on a 'top down' and 'bottom up' approach:
- The 'top down' approach involves the executive and senior leadership teams, identifying and managing the risks that we face in achieving our strategic and business objectives. These risks form our corporate and sub risks.
- The 'bottom up' approach focuses on engaging employees at all levels, including frontline and site staff throughout SBC in identifying and managing risks. These risks form our 'business' risks.

The risk management approach will be followed at all levels of the Council as shown in diagram 1 below:

Top Down/Bottom-Up Approach

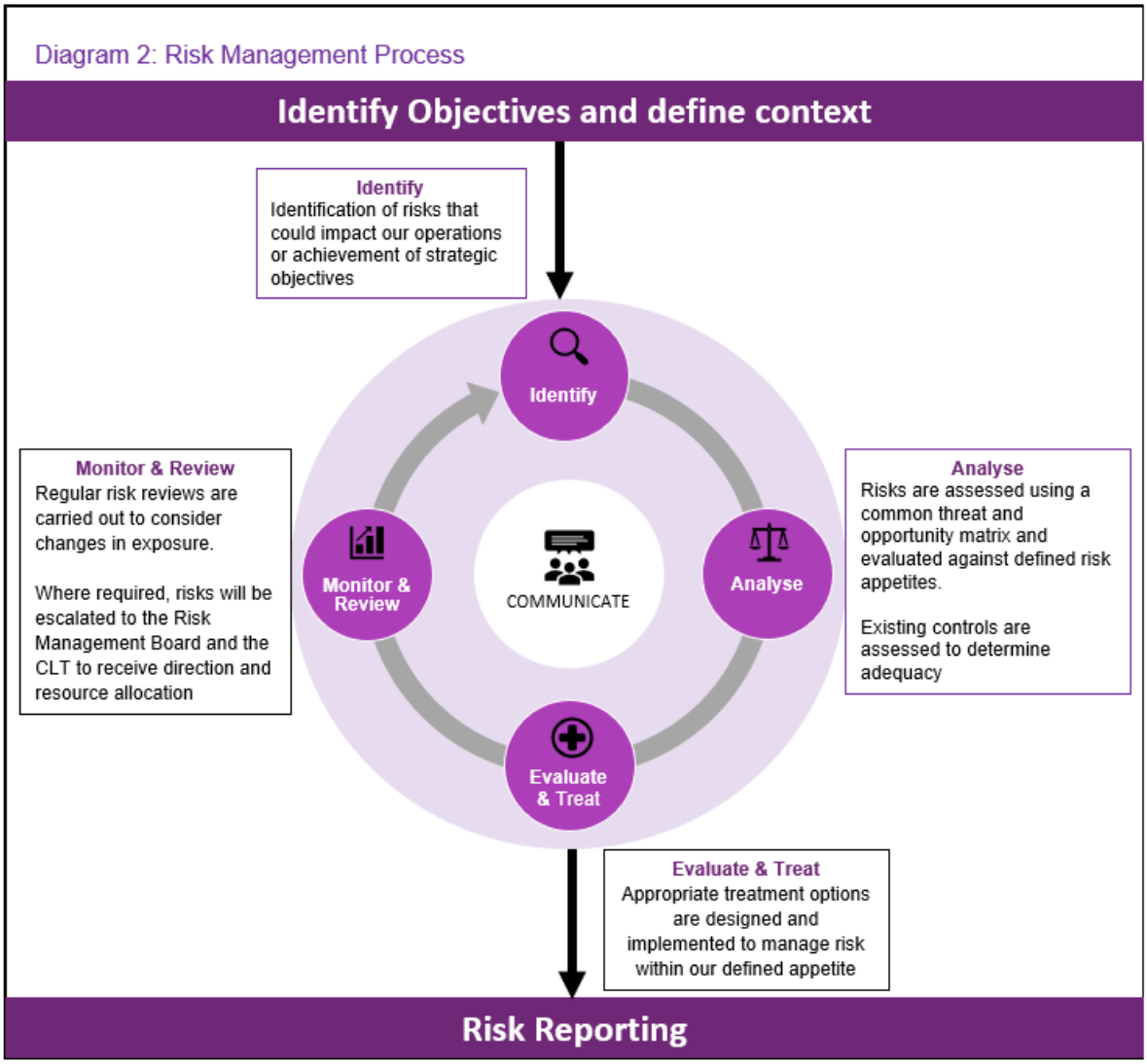


3.04 Risk Management Process

Our risk management process details below the overarching mandated requirements for the whole business.

As shown in diagram 2 below, risk management is shown as a continuous process, supplemented at the start by identifying business aims and objectives and later through reporting, both internally and externally, on the Council's risk profile.

Diagram 2.



Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

It should be conducted systematically, iteratively, collaboratively and drawing on the knowledge and views of stakeholders. It should use the best available information, supplemented by further enquiry as necessary.

3.05 Identify

The purpose of risk identification is to identify and describe risks that might help (opportunity) or prevent (threat) us from achieving our objectives. We should consider the full range of risks the council faces, including risks that we are exposed to during operational delivery and those that could have an impact on the achievement of strategic objectives.

Whenever, there is a change in the strategy, objectives or business processes, existing risks shall be reassessed, and any new risks identified shall be assessed.

Identifying and addressing material risks is a key aspect of effective risk management, ensuring that resources are allocated appropriately to manage the most critical challenges facing the Directorate/Division and ultimately, SBC.

For example:
Impact day to day business operational objectives, (i.e., compliance with standards, contractual and statutory obligations)

- Impact delivery of the council's long term/strategic objectives (i.e., failure to become a 'best value council', building resilient assets and systems, optimising technology innovation and sustainable practices, for example)
- Are of concern to stakeholders (i.e., non-delivery of our commitments, not meeting regulatory obligations.)

3.06 Describing risks

Risks can be identified through strategic planning, business planning, project initiation, horizon scanning and the ongoing assessment of the organisation's work. Once objectives are understood, risks which may impact them shall be identified and described clearly so that stakeholders can understand the **'risk event'** (i.e., what might happen**); the 'root causes'** (i.e., why it might happen); and the '**consequences**' (i.e., impacts if it happens).

Example of describing a risk:

The **'root cause'** of the risk	*due to inadequate financial checks...*
The risk **'event'**	***...** A staff member commits fraud...*

The **'consequence'** of the risk (as it relates to objectives)	*...resulting in monetary loss to the organisation*

3.07 Emerging risks

Emerging risks are those that are newly developing or rapidly changing and therefore their extent and implications are not fully understood. As such they cannot be fully assessed in the same way as our current risks however, they do have the ability to affect the future viability of SBC if appropriate steps are not taken to understand and respond accordingly. Therefore, as part of our risk management process, on a monthly basis consider changes in our operating landscape and the subsequent emerging risks that could arise over the short, medium and long-term timescale.

Directorates identify emerging risks through horizon scanning, engaging with risk champions and other people in the business who are engaged with external bodies and forums. Emerging risks are captured in the 'Emerging Risk Summary Template' and reviewed by the risk and insurance team against existing risks. The risks are shared with affected teams and an overview shared with the risk champion for inclusion in quarterly risk reviews and captured in the risk registers with detail and assessment undertaken as the relevant information comes available.

The emerging risk template can be found at *appendix 4.05 Emerging risk template*

3.08 Cross functional approach

It is important that directorates/departments do not operate within silos when identifying and assessing their risks but ensure that they work with any other areas of the business who are facing the same risks.

Cross-functional risk management is an approach that involves collaboration across various directorates/departments within the council to identify, assess, and manage risks. As an example, while identifying and assessing a risk it may be necessary to speak to a number of stakeholders either individually or ideally in a group, from different functions for example finance, adults, people, and DDaT, to allow risk ownership to be assigned based on the impact on each business unit and captured in the relevant risk registers, which will ensure a comprehensive management of the identified risk. Regular meetings should be held to monitor the management of the risk, review risk statuses, and adjust plans as necessary. Effective communication and collaboration are key throughout the process, ensuring that all stakeholders are informed and aligned on the risk management objectives and actions.

Cross-functional risk management matters because it helps you align your efforts and resources with your vision and objectives. It also enables you to respond to any changes due to internal or external influences. By managing cross-functional risks

effectively, we will enhance the identification and management of risks which will optimise resource allocation and improve overall management of risks.

3.09 Analyse

The purpose of risk analysis is to comprehend the nature of risk and its characteristics including the level of risk. Risk analysis involves assessing the causes and resultant consequences of risk events affecting objectives. An event can have multiple causes and consequences and can affect multiple objectives. Controls should be identified, and their effectiveness taken into consideration.

Risk analysis should consider factors such as:

- the likelihood of events and consequences
- the nature and magnitude of consequences
- complexity and connectivity
- time-related factors and volatility
- the effectiveness of existing controls

The level of detail with which risk is analysed may vary depending on the nature and materiality of the risks identified.

Risks shall be assessed/scored using the SBC Risk Assessment Matrix, which considers eight impact criteria and the scale of probability of it occurring, see *Appendix 4.02 Risk Assessment Matrix.*

The Council has historically used a risk heat map to visually represent risks by multiplying impact and likelihood, to generate an overall risk score, with colour-coding to indicate risk levels. This method offers a snapshot of the corporate risks.

However, the multiplication approach can be misleading. Score of 25 and 5 differ greatly in value, but both could have catastrophic consequences. Low-likelihood (rare), very high-impact events may receive too little attention, despite their potential to occur. Additionally, this method suggests that a moderate-impact, possible event with a score of 9 is more deserving of management attention than a very high-impact, low-probability event scoring 5, which is not necessarily accurate.

To improve clarity, we plot impact and likelihood on the heat map matrix, which reflects a scale of relative importance. Box 25 is the most significant, followed by 24, 23, and so on. In this approach, very high impact, low-likelihood risks score 15 (instead of 5), providing a more accurate representation of risk. This also shows that such risks score higher than moderate-impact, possible events (15 vs. 13), offering a clearer assessment.

The impact and likelihood scores for risk events shall be evaluated at two points:

- **Current risk score** - this is the level of risk we consider we are exposed to 'today', taking into consideration the existing controls that are in place to manage the risk. It serves as a dynamic indicator that aids in prioritising and addressing risks in the current state of operations.
- **Target risk score** – acceptable future level of risk that aligns with organisational risk appetite which will be achieved by the delivery of treatment/mitigation plans.

IMPORTANT
Scoring risks involves a pragmatic evaluation of the impact and likelihood that leans towards a reasonably foreseeable worst case impact estimate rather than fixating on the extreme scenarios.

The risk score will determine which level of severity the risks sit in. There are four risk levels (Red, Amber, Yellow or Green), which classify the significance of the risk and guide the urgency of action required. See table 1 below.

Table 1 – Risk Severity

Red (20 – 25)	Red risks are high-impact, high-likelihood risks that pose a severe threat to our objectives, operations, or strategic initiatives. These risks require immediate attention and robust treatment/mitigation strategies.
Amber (15 – 19)	Amber risks indicate that our objectives may not be achieved. Appropriate treatment/mitigation strategy to be devised as soon as possible.
Yellow (7 – 14)	Yellow risks indicate that our objectives may not be achieved. Appropriate treatment/mitigation strategy to be devised as part of the normal risk management process
Green (1 – 6)	Green risks represent low-level concerns that are manageable and unlikely to significantly affect our objectives.

The majority of management focus and further risk treatment/mitigation should be focused on Red and Amber risks.

3.010 Controls

Controls are specific measures, actions, policies, procedures or mechanisms put in place to manage a risk and are designed to minimise the likelihood and or impact of potential threats occurring.

3.011 Evaluate & Treat

Evaluate

Risk analysis should be evaluated against defined risk appetites, to identify risk within and outside of tolerance and levels of acceptability. This will support decisions on the management of the risk, including the prioritisation and treatment.

Risk appetite is the level of risk SBC is willing to seek or accept in pursuit of achieving its long-term objectives and creating value. Risk appetite guides resource allocation and provides the means to effectively respond to and monitor risks.

The following scale represents the approach used by SBC for assessing risk appetite.

See table 2 below:

Table 2

Risk averse (Conservative)	Risk balanced		Risk seeking (entrepreneurial)
No or very low tolerance - with a preference for conservative strategies with negligible or low risk. Applying innovation prudently where the risks are fully understood.	Low tolerance - willing to accept a small degree of risk but aim to reduce exposure where possible. Applying innovation only where successful delivery is likely.	Medium tolerance - willing to take risk where the risk/reward ratio is deemed acceptable. Applying innovation only where successful delivery is likely.	High tolerance - a willingness to take on higher levels of risk in pursuit of greater rewards. Eager to be innovative and exploit opportunities.

Treat (mitigate)

Once risks have been identified, analysed and evaluated, the next step is to decide what to do about them.

For all current risks (the remaining exposures after existing controls have been considered), management shall decide upon, and explicitly document, a risk treatment selected from one of the following options:

Treat	take action by implementing controls in order to reduce the likelihood of the risk developing and/or limiting the impact to acceptable levels.
Tolerate	retain the risk by making an informed decision (do not introduce new controls or treatments)
Transfer	share the risk with another party e.g. insurance, contracts, third parties.
Terminate	remove the risk source by ensuring that measures are in place to either stop the risk from occurring or preventing the risk from having any impact

Selecting the most appropriate option involves balancing the costs and efforts of implementation against the benefits derived.

Risk treatment can also introduce secondary monitor risks which must be captured and managed.

3.012 Monitor and Review

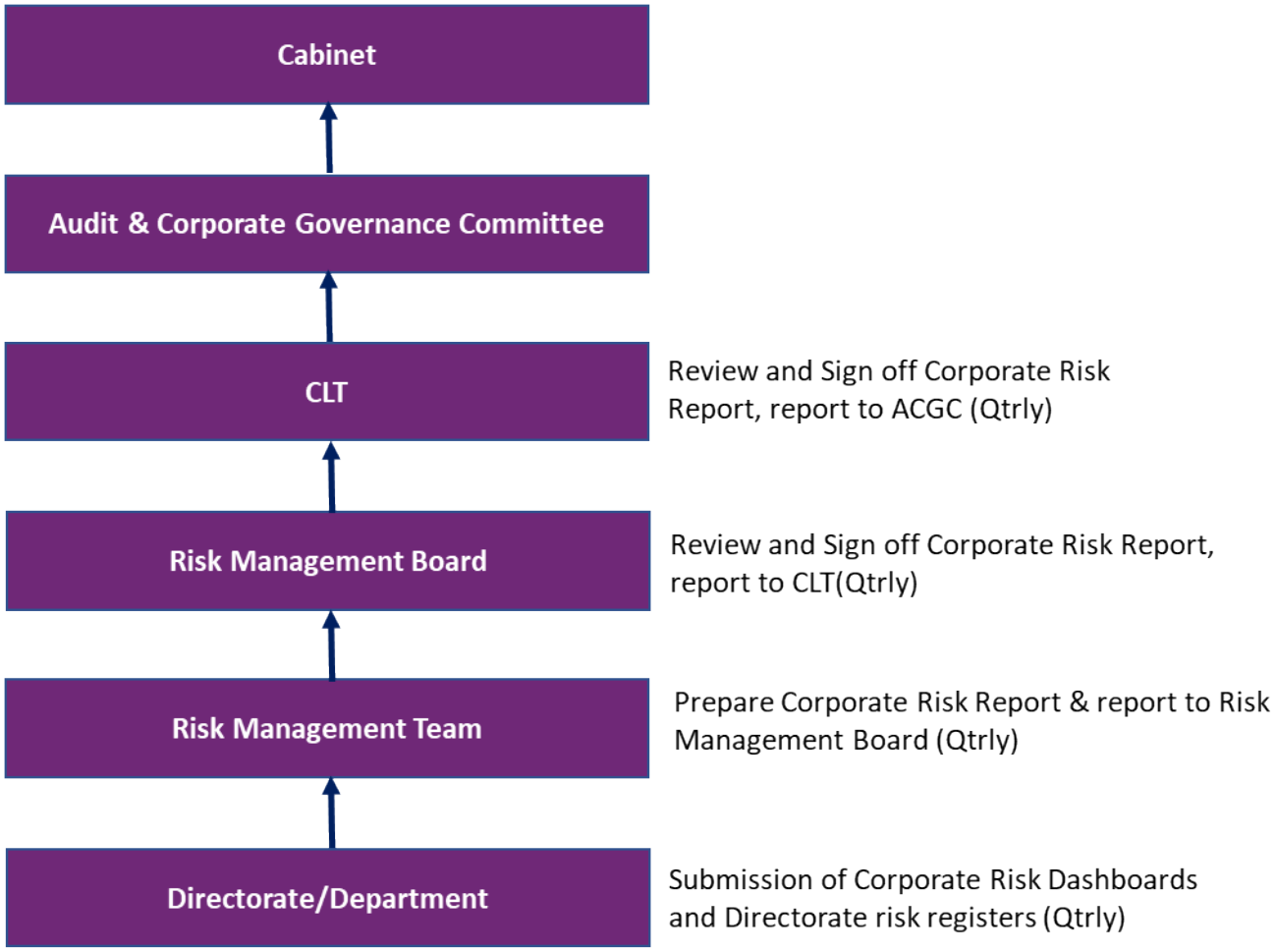
Ongoing monitoring and periodic review of the risk management activity and its outcomes should be a planned part of the risk management process to ensure that the treatment action taken, and the controls put in place are effective in managing the risk. Reviews must consider movements in the exposure of existing risks and include identification of new or emerging risks.

As a minimum the following review periods will be followed:

- Council - Annually
- Audit & Corporate Governance Committee – Quarterly
- CLT – Quarterly
- Risk Management Board– Quarterly
- Corporate Risk Dashboards – Quarterly
- Directorate/Department Risk Registers – Quarterly

These review periods are driven by our risk governance process depicted below:

RISK GOVERNANCE PROCESS



At the risk owner's discretion more frequent reviews are encouraged particularly for the highest scoring risks (Red risks) and any rapidly changing risks. Additionally, risk reviews of material risks should be a standing agenda item on monthly Leadership Team (DLT) meetings.

The material risks are typically prioritised for focused monitoring and mitigation efforts as they have the potential to significantly influence the overall success of the Directorate/Department and therefore need to be reviewed by the relevant Senior Leadership team.

We define a material risk as having a significant material impact i.e. with an impact score of **5** or with a current risk score of **18** and above, using the SBC Risk Assessment Matrix. Any outlying risks, low likelihood, high impact, should also be considered on a regular basis.

The various monitoring mechanisms for risks will include the following:

- Identified controls and their effectiveness
- Identified roots causes and consequences have not changed
- Quarterly evaluations of impact and likelihood

If the status of risk treatment plans (milestones & delivery dates) deteriorates, particularly those of material and corporate risks, this must be communicated to the relevant Risk Champions, Risk Owner and Risk Management team for proactive and corrective actions to be taken. If deemed necessary, it should also be escalated to the Risk Management Board.

Risk champions must take recognition of the fact that risks may evolve over a period of time. Hence, a monthly/quarterly review of the treatment activities must be implemented to ensure that the action plan remains on time

3.013 Risk Reporting

The risk management process and its outcomes should be documented and reported through directorate risk registers and corporate risk dashboards.

3.014 Risk Recording

Flow of Risk Information
This section describes the flow of risk information from departmental level up to the CLT as well as the filtration process in between:

1. The first level will be conducted by the departments. Once risks are assessed by departments and directorates, only the material risks are escalated to each DLT through the respective directorate Risk Champions.
2. The Risk Management team will act as a second level of filtration of risks.
3. The Risk Management team will consolidate the directorate risk registers and produce a report on a quarterly basis.
4. The Risk Management Board will be responsible for assisting SBC in its oversight of corporate risks of the Council

Risk Profiling
SBC will develop risk registers at divisional and departmental level. The purpose of the risk register is to identify, prioritise, and assign ownership for risks that create uncertainty around the achievement of directorate and divisional objectives

Each risk register will contain a set of key risks with the following details:

1. A description of the risk, together with the associated root causes and consequences

2. A current risk rating based on the assessment results (identified likelihood and impact of the risk)
3. Current controls in place to manage the risk and the effectiveness of the controls in place.
4. Treatment action, if any and expected due dates.
5. Ownership of the risks and treatment plans

To ensure an accurate representation of the risks in the risk register, Risk Champions and directorate heads will sign off their directorate risk register on a quarterly basis.

The Risk Management team will arrange to meet and review the directorate risk registers at least on a quarterly basis. The objective of the meetings will be to assess and review the risks and as well as mapping to the corporate risk dashboards.

A quarterly Corporate Risk Report based on the corporate risk dashboards will be reviewed and approved by the Risk Management Board then submitted to the CLT for final approval before being submitted to the Audit Committee.

3.015 Frequency

The below is an indicative timeline of the risk management activities:

Indicative timing	Key activities	Formal report
Monthly	Directorates/Divisions review for emerging and/or current risks	Risk Champions communicate any identified emerging risks to the Risk Management team
Quarterly	Directorates/Divisions review risk registers and undertake a risk assessment update exercise	DLT sign off Directorate risk register
Quarterly	Risk Management team reviews Corporate Risk Dashboards and produce the quarterly Corporate Risk Report.	Quarterly Corporate Risk Report approved by the Risk Management Board
Quarterly	Risk Management team presents quarterly Corporate Risk Report to CLT	Corporate Risk Report approved by CLT, then submitted to the Audit Committee
Annually	Corporate risk assessment exercise with the CLT	Corporate risk profile approved by the CLT

3.016 Risk Registers

All directorate/departmental risks must be recorded in a risk register, see Appendix 4.01.

Each risk must be assigned a risk owner with the appropriate seniority and delegated authority to be accountable for the management of the risk.

Risk Owners are responsible for:

- Ensuring their risks are properly understood and articulated.
- Risk assessment (including scoring and controls)
- Reviewing control effectiveness
- Introduce treatment/mitigation plans when required and monitoring their implementation.
- Reviewing their risks on a regular basis

As well as an assigned risk owner, risks should also have a risk lead/ responsible person to act as a subordinate for risk owner. Also action owners and control owners are identified.

Action Owners are responsible for:

- Ensuring that the mitigation/treatment actions under the treatment plan are implemented within any specified parameters e.g., time and cost.
- Providing regular updates to the Risk Owner on the progress and effectiveness of the actions and undertake changes as directed by the Risk Owner

3.017 Risk Escalation: A Bottom-Up Perspective

A well-structured risk escalation framework ensures that significant risks are properly identified at operational levels and effectively communicated upward through the organisation. Here's how risks are escalated through our system from the bottom up:

Departmental Risk Identification

At the departmental level, teams identify and assess risks specific to their operations using the 1-25 scale. Each risk receives:

- An impact score (1-5)
- A likelihood score (1-5)
- An overall risk score (Plotting impact & likelihood on risk map)

Department managers maintain their risk registers, regularly reviewing and updating them to reflect current conditions.

Risk Escalation Criteria

Based on your framework, risks qualify for escalation when they meet either of these conditions:

- Overall risk score of 18 or higher
- Impact score of 5 (regardless of likelihood)

These thresholds ensure that both high-probability risks and potentially catastrophic events receive appropriate attention, even if their likelihood is low.

Escalation to Directorate Level

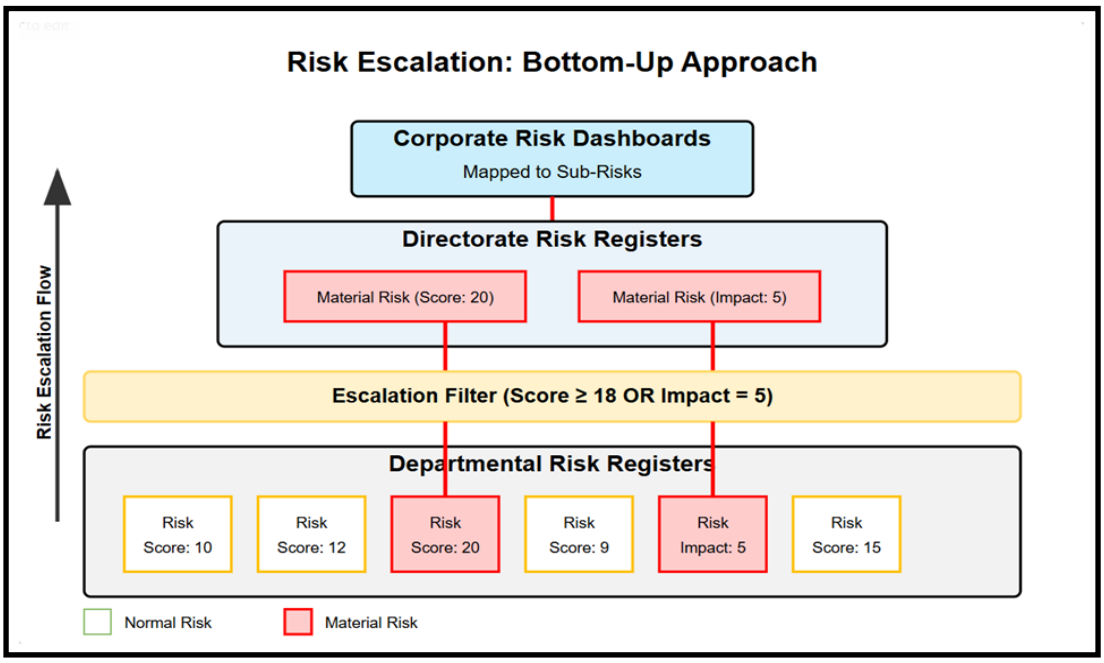
When departmental risks meet the escalation criteria:

1. They are flagged in the departmental risk register
2. Details are communicated to the relevant directorate
3. The risk is recorded in the directorate's risk register
4. Directorate-level risk mitigation strategies are developed
5. At this level, similar risks from multiple departments may be aggregated or linked to show systemic issues.

Mapping to Strategic Risks

Material risks from directorates are then mapped to the Sub-Risks of the Corporate Risk Dashboards. This process:

1. Connects operational concerns to strategic objectives
2. Provides senior leadership with visibility of significant threats
3. Enables enterprise-wide risk management decisions
4. Ensures resource allocation aligns with the organisation's most critical risks



Benefits of the Bottom-Up Approach

This escalation framework ensures that:

- Risks are identified by those closest to operations
- Nothing significant falls through the cracks
- Decision-makers have appropriate visibility of material risks
- The organisation maintains a comprehensive view of its risk landscape

Regular review cycles at each level maintain the system's effectiveness, ensuring timely identification and management of emerging risks.

3.018 Risk Management Board and CLT Committee Reporting

Our Corporate Risks are owned by members of the CLT and are reviewed by the Risk Management Board, and the Audit & Corporate Governance Committee on a quarterly basis. These risks are recorded in the Corporate Risk Dashboards, see *Appendix 4.03*

The risk management team produce the relevant risk reports and dashboards for these committees in collaboration with the business, to provide oversight of the material risks to the council (the overall council risk profile) and to show how these risks are being managed, as well as information on new and emerging risks.

www.slough.gov.uk
Slough Borough Council

Growing a place of opportunity and ambition

4.0 APPENDICES

4.01 Risk Register Template *(Link)*

All material risks that;
1) possess a level of significance requiring attention and management due to their potential to affect our financial performance, reputation, operations, or strategic goals. (classified by our strategic, financial, compliance and operational risks)
2) Risks with an impact score of 5 or with a current risk score of 20 or above, using the Risk Assessment Matrix.
NOTE: LINE 4 (YELLOW HIGHLIGHT) IS AN EXAMPLE, AND SHOULD BE DELETED ONCE YOU START TO POPULATE YOUR REGISTER

Risk Ref: DIR specific	Directorate	Function	Threat / Opportunities	Risk Title (risk event)	Risk Description (causes, risk event, consequences)	Risk Owner	Risk lead/ Responsible person	Risk Status (New, Open, Closed)	Categories (Strategic, Operations, Financial, Compliance)	Corporate Risk mapping	Sub-Risk Mapping
FC 1	Finance & Commercial	Insurance	Threat	EXAMPLE Failure to secure insurance for certain classes	EXAMPLE Due to our history of claims and magnitude of potential claims there is a risk of failure to secure insurance for certain classes	John Smith	Ann Black	Open	Financial	CR_03_Financial_Sustainability	

CURRENT RISK SCORE										To include a new line use ALT, Return buttons			
Overall Current Risk Score	Likelihood Score	Highest Impact Score	Environmental Impact Score	Legal & Political, Compliance Impact Score	IT Systems/Cyber/GDPR Impact Score	Health & Safety Impact Score	People Impact Score	Service Delivery Impact Score	Reputation Impact score	Financial Impact score	Control Effectiveness (See tab for definition) evaluate all identified controls for overall control effectiveness	Control Owner	Control Description	Control Title
	3	5	0	0	0	0	0	2	5	4	Needs improvement	Ann Black	1. Ongoing monitoring of claims value/volume	1. Claims monitoring

Risk Response (4 T's) Treat, Transfer, Tolerate, Terminate	Treatment/Mitigation title (Title & completion date)	Treatment/mitigation description	Owner	Status (Align status with Not started / On track / Delayed no mitigation / Delayed with mitigation / Completed)	Financial Impact score	Reputation Impact score	Service Delivery Impact Score	People Impact Score	Health & Safety Impact Score	IT Systems/Cyber/GDPR Impact Score	Compliance, Legal & Political Impact Score	Environmental Impact Score	Highest Impact Score	Likelihood Score	Overall Target Risk Score	Business Continuity Plans	Comments (include delivery variance, dependencies etc)
To include a new line use ALT, Return buttons					TARGET RISK SCORE												
Treat	1. Captive feasibility study Completion date: (31/01/2024) 2. Plan to move to a Captive insurance arrangement Completion date: (01/04/2025)	1. Set up and undertake Captive feasibility study, which would ensure continuity of securitisation requirements 2. Should insurance be declined or cost prohibitive at point of renewal, 'warm' plan in place to move to a Captive instance arrangement	1. Joe Bloggs 2. Joe Bloggs	1. On track 2. Not started	3	2	0	0	0	0	2	0	3	3	13	No	Last update Position continues to be monitored Working with Broker on feasibility study

Directorate Risk Register | Risk Assessment Matrix | Control Effectiveness Defn | Heatmap | Corporate & Sub-Risks

Risk Assessment Matrix

	IMPACT				
CATEGORIES	**1 - Very Low**	**2 - Low**	**3 - Moderate**	**4 - High**	**5 - Very High**
Financial Impact Budget overruns, loss of funding, or significant unforeseen expenses.	Up to £100,000	Between £100,000 - £500,000	Between £500,000 - £1,000,000	Between £1,000,000 - £10,000,000	In excess of £10,000,000
Reputation Damage to the council's public image or loss of trust among the community	Minor/ no negative media coverage or impact on the way the council is perceived by local community Negative social media publicity on minor channel(s), 6 days or less	Local negative media coverage and impact on the way the council is perceived by local community, with a reasonable opportunity to rectify Negative social media publicity on a number of minor channels, 7 days or more	Local and national negative media coverage and impact on the way the council is perceived by local community, with a reasonable opportunity to rectify Negative social media publicity on a single mainstream channel, 7 days or more	Widespread local and national negative media coverage and impact on the way the council is perceived by local community, with some effort required to rectify Negative social media publicity on a single mainstream channel, 7 days or more	Widespread local, national and international negative media coverage and impact on the way the council is perceived by local community, with no guarantee this can be rectified Extended negative social media storm, multiple mainstream channels (Facebook, X etc) : 7 days or more
Service Delivery Disruption or failure in delivering critical services to the public.	Minimal or no noticeable impact on service delivery	Some disruption to non-critical services, but essential services remain unaffected	Noticeable disruption to important services, but core or critical services continue to function.	Significant disruption or failure of critical services, resulting in major service delays or reduced availability	Complete or near-complete failure of essential public services with severe consequences for the community
People	Negligible reaction for employees within one key function Loss of operation - critical personnel between 1%-3%	Moderate adverse reaction from employees across more than one key function Loss of operation - critical personnel between or less than 3%-5%	Major loss of confidence and support from employees within more than one key function Loss of operation - critical personnel of less than 5%	Significant loss of confidence and support from employees within more than one key function Loss of operation - critical personnel between 5%-15%	Overwhelming loss of confidence and support from majority of employees Loss of operation - critical personnel of more than 15%
Health and Safety Risk of injury, illness, or death to employees, the public, or stakeholders	Near miss incident Individual public health incident	RIDDOR/ Reportable Lost time incident (LTI) Localised public health incident	Long term disability, life changing physical or mental health injury Widespread public health incident	Fatality/multiple life changing injuries Serious localised public health incident (e.g. hospitalisation)	Multiple fatalities with potential to lead to criminal prosecution Serious widespread public health incident
IT Systems/Cyber/GDPR Breaches, data loss, or IT system failures affecting operations or data privacy	No system outages No system vulnerabilities disrupted by malicious actors Data breach is unlikely to result in a risk to the rights and freedoms of individuals (e.g. identity theft, reputational damage, impact to career etc)	No disruption to operations with some non-critical system outages Minimal system vulnerabilities disrupted by malicious actors, with an ability to recover Data breach could possibly result in a risk to the rights and freedoms of individuals (e.g. identity theft, reputational damage, impact to career etc)	Minor disruption to operations with some critical system outages, or significant non-critical system outages Some system vulnerabilities exploited by malicious actors, with an ability to recover in most cases Data breach is likely to result in a risk to the rights and freedoms of individuals (e.g. identity theft, reputational damage, impact to career etc)	Some disruption to operations with outage of numerous critical systems Significant system vulnerabilities exploited by malicious actors, with an ability to recover in most areas Data breach is likely to result in a risk to the rights and freedoms of individuals (e.g. identity theft, reputational damage, impact to career etc). Notification to the supervisory authority (ICO) is needed and non-financial reprimands are imposed	Extensive outage of critical systems with the business unable to operate Significant system vulnerabilities exploited by malicious actors, with no ability to recover Data breach is likely to result in a high risk to the rights and freedoms of individuals (e.g. identity theft, reputational damage, impact to career etc). Notification to the supervisory authority (ICO) which may result in financial and/or non- financial reprimands and we are required to inform the impacted data subjects
Compliance, Legal & Political Breach of laws, regulations, or statutory requirements	(Voluntary) notifiable Regulator non- compliance - Breach resolved between parties	Notifiable Regulator non- compliance - Formal RFI / Third party concern and dissatisfaction / material operational issues emerge publicly	Legal/regulatory action, regulator enforcement penalties / repeated major stakeholder enquiries / repeated failure to deliver against regulatory commitments	Severe regulatory action/ prosecution criminal/ negligent behaviour / trust issues leading to extreme financial or regulatory consequences.	Major litigation that cannot be defended. Critical breach of legislation, possibility of significant (quantify) fines / imprisonment of officers / members
Environmental	Minimal short-term/temporary environmental damage	Borough-wide environmental damage	Major long term environmental damage	Very severe long term environmental damage	Irreversible and significant environmental damage

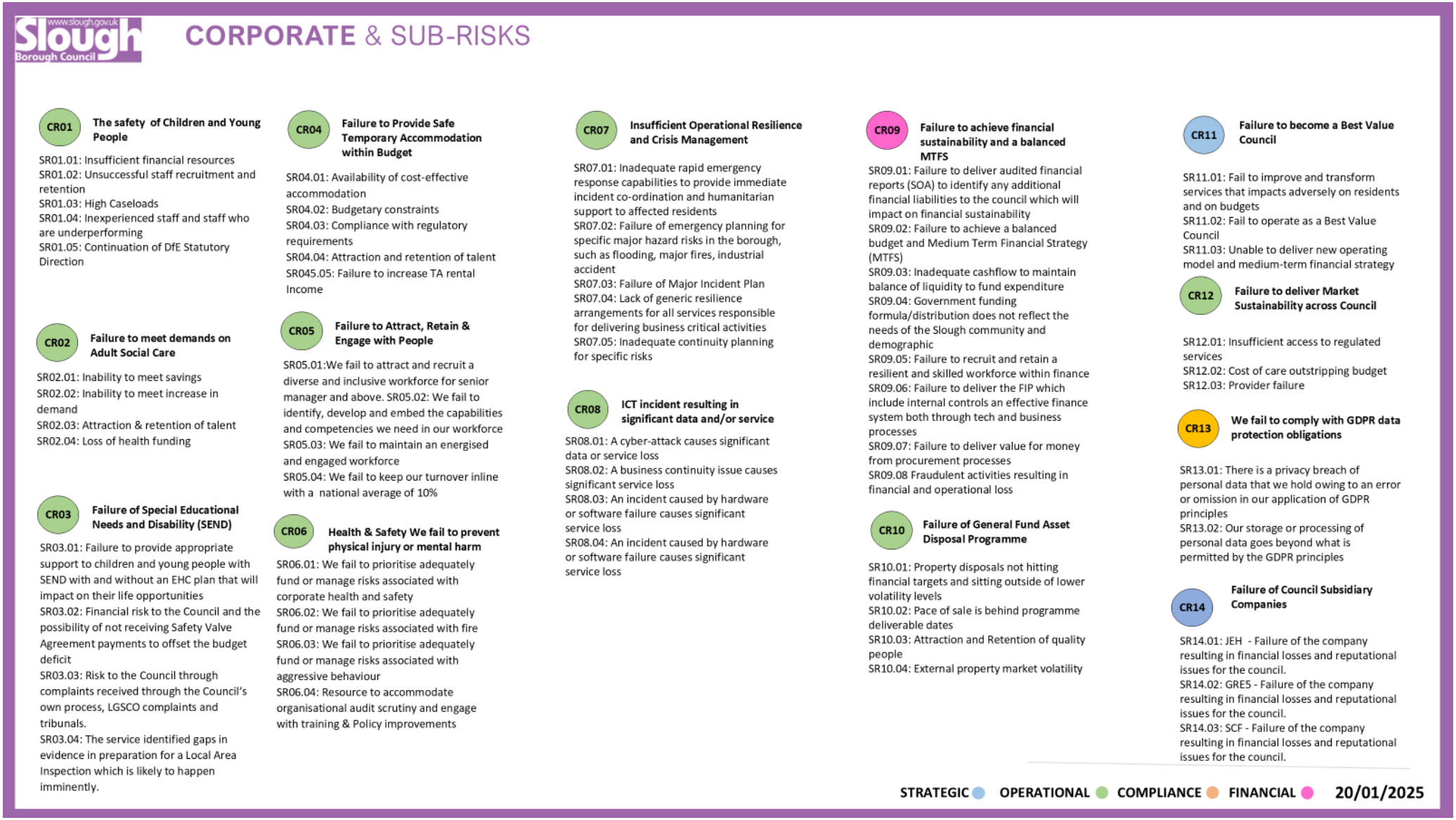
Likelihood				
1 – Rare	**2 - Unlikely**	**3 - Possible**	**4 - Probable**	**5 - Almost Certain**
Event will occur only in exceptional circumstances. No past event history (SBC or UK public sector)	Event could happen in the next 3 - 5 years. Some past history exists (SBC, or UK public sector)	Event could happen in the next 1-2 years. Past history of event circa every 1-2 years (SBC or UK public sector)	Event could happen in the next 7-12 months. Recurring past event e.g. annually (SBC or UK public sector)	Event could happen in the next 0-6 months.

How to Use the Matrix

1. Identify the Risk: Define the potential risk within one or more of the impact categories.
2. Determine Likelihood: Estimate the likelihood of the risk occurring using the 1-5 scale.
3. Assess Impact: Determine the severity of the impact using the 1-5 scale.
4. Calculate Risk Score: On the heat map, take your separate impact and likelihood scores and plot on the x & y axis to obtain your risk score. This will be a number between 1 - 25
5. Prioritise Actions: Use the risk score to prioritise risk mitigation efforts, with higher scores requiring more immediate action.

4.02 Risk Assessment Matrix *(Link)*

4.03 Corporate & Sub Risks/ Sample Corporate Risk Dashboard Template – as at 20/01/2025



4.04 Corporate Risk Dashboard – SAMPLE *(Link to blank template)*

CR20	Cybersecurity Risk	Risk owner:Executive Director

Corporate risk overview

Current Risk Score 5 Impact 4 Likelihood	24
Target Risk Score 4 Impact 3 Likelihood	18

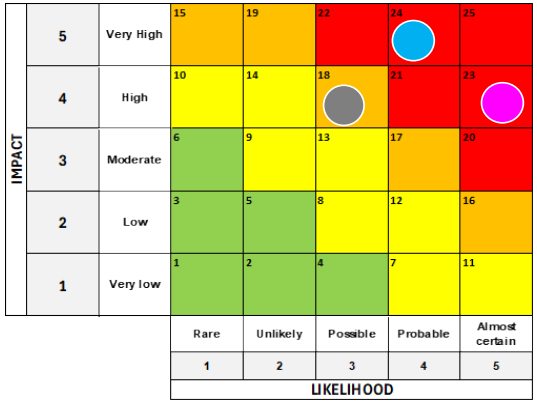
RAG status: Overall risk remains at HIGH (RED) due to increasing cyber threats and sophisticated attack vectors targeting our sector
Biggest exposures: Remote working infrastructure, legacy ERP system[illegible]ilities, and third-party integrations
Current incidents, concerns: 3 successful phishing attempts blocked, [illegible]tem[illegible]d ransomware attack contained, concerns over staff security awareness
Internal or external themes: Increase in sector-specific cyber at[illegible]ks, ne[illegible]egulatory requirements (NIS2 Directive), hybrid working model creating expanded attack surface
Emerging risks: AI-powered cyber attacks, supply chain compromise[illegible]ntum c[illegible] threats to current encryption

Risk appetite statement (Averse/Balanced/Seeking) Choose

Averse - Low tolerance for cybersecurity risks given potential for severe reputational damage, regulatory penalties, and operational disruption. Conservative approach preferred with comprehensive security controls

SAMPLE

Risk profile



Refer to slide 7 for risk assessment score instructions

Sub risks related to this [illegible]l ris

Ref	Status	Risk title	Sub-risk owner	Change in period / outlook	Management Review/ Explanation of movement
14.01		Data Breach & Privacy Violations	David Ch[illegible] InfoSe[illegible] Man[illegible]		Increased phishing attempts targeting remote workers. Two near-miss incidents this quarter. Enhanced security awareness training implemented
14.02		System Infrastructure Vulnerabilities	M[illegible] Johns[illegible] IT Director		Legacy systems upgrade 60% complete. Critical patches applied quarterly. Network segmentation project on track.
14.03		Third-PartyVendor Security	Lisa Smith Procurement Director		New vendor security assessment framework implemented. 85% of critical vendors now compliant with security

4.05 Risk Heatmap *(Link)*

IMPACT							
	5	Very High	15	19	22	24	25
	4	High	10	14	18	21	23
	3	Moderate	6	9	13	17	20
	2	Low	3	5	8	12	16
	1	Very low	1	2	4	7	11
			Rare	Unlikely	Possible	Probable	Almost certain
			1	2	3	4	5
			LIKELIHOOD				

The Council has historically used a risk heat map to visually represent risks by multiplying impact and likelihood, to generate an overall risk score, with colour-coding to indicate risk levels. This method offers a snapshot of the corporate risks.
However, the multiplication approach can be misleading. Score of 25 and 5 differ greatly in value, but both could have catastrophic consequences. Low-likelihood (rare), very high-impact events may receive too little attention, despite their potential to occur. Additionally, this method suggests that a moderate-impact, possible event with a score of 9 is more deserving of management attention than a very high-impact, low-probability event scoring 5, which is not necessarily accurate.
To improve clarity, we no longer multiply scores. Instead, we plot impact and likelihood on the heat map matrix, which reflects a scale of relative importance. Box 25 is the most significant, followed by 24, 23, and so on. In this approach, very high impact, low-likelihood risks score 15 (instead of 5), providing a more accurate representation of risk. This also shows that such risks score higher than moderate-impact, possible events (15 vs. 13), offering a clearer assessment.

4.06 Emerging risk template *(Link)*

www.slough.gov.uk
Slough Borough Council
Growing a place of opportunity and ambition

EMERGING RISK SUMMARY TEMPLATE

PREPARED BY:

RISK ISSUE:		
WHAT IS HAPPENING RIGHT NOW?		
WHAT FACTS DO WE CURRENTLY KNOW?	WHAT DO WE CURRENTLY NOT KNOW?	HOW MIGHT THIS RISK IMPACT OUR ORGANIZATION?
HOW FAST IS IT MOVING?	WHAT SEEMS TO BE DRIVING THIS RISK?	
WHAT DATA CAN WE TRACK TO MONITOR THIS RISK?		
WHAT RESPONSES DO WE HAVE IN PLACE?		WHAT ELSE SHOULD WE CONSIDER?

4.07 RACI Matrix

The RACI (Responsible, Accountable, Consulted, Informed) matrix links key risk management activities to SBC primary risk management roles and establishes the level of accountability for each activity. SBC primary risk management roles are either:

- **E** = **Execute** – Responsible (responsible for performing the activity)
- **O** = **Owner** – (accountable for making the business decision and its outcome or delegating specific tasks to other employees or teams)
- **C**= **Consulted** – Consulted (consulted for inputs and feedback; however, agreement or action on input is not required)
- **I** = **Informed** – Informed (informed of the final result, task completion, or deliverable distribution)
- **F**= **Facilitate** – Facilitate the performance of the activity or task
- **M** = **Monitor** – Monitor (monitors to ensure that the activity is being addressed)

Process	Activity	Risk Owner	Risk Champion	Risk & Insurance Manager	Risk Management Board	Corporate Leadership Team
Governance	Develop RM programme (framework, policies and procedures)			**E - O**	**C**	**I - M**
	Approve risk management policies			**E**		**O**
	Update and maintain RM Strategy document			**E - O**	**C**	
Risk Identification	Identify New and Emerging Risks	**O**	**C – M**	**C, F**		
	Review each risk in existing directorate register and confirm its validity, root causes and consequence	**O**	**E**	**C**	**C**	

Process	Activity	Risk Owner	Risk Champion	Risk & Insurance Manager	Risk Management Board	Corporate Leadership Team
	Update directorate Risk Register	O	E	F		
Risk Assessment	Review and update Divisional risks' impact and likelihood	O	E	F		
	Review and update the impact and likelihood of risks that arise at corporate level only			F	E	M
	Review the top corporate risks			F	C	M
Develop Risk Response	Review current treatment strategies for top corporate risks	O - E	F	C		M
	Review treatment strategies for top directorate risks	O - E	F	C	M	
	Validate current treatment strategies for top corporate risks	E - O	F	C		
Implement Risk Response	Implement SBC risk treatment strategies	O - E	F	C		
	Implement divisional risk treatment strategies	O	F	C		
Risk Monitoring and Reporting	Prepare SBC risk reports			E - O	I	I
	Prepare directorate risk reports		F	E - O	I	

Process	Activity	Risk Owner	Risk Champion	Risk & Insurance Manager	Risk Management Board	Corporate Leadership Team
	Monitor top QR risk	O - E	O - E	F	C	F
	Monitor top divisional risks	O	E	F		

4.08 Glossary of Terms

Slough Borough Council has adopted the following glossary of terms that are aligned with ISO 31000:2018, to establish a uniform and consistent risk management programme across the Council:

Risk	The effect of uncertainty on objectives - The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of likelihood and impact
Risk Management Framework	A set of components that provides the foundations and Council arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the Council. The foundations include the policy, objectives, mandate and commitment to manage risk. The Council arrangements include plans, relationships, accountabilities, resources, processes and activities. The risk management framework is embedded within the Council 's overall strategic and operational policies and practices.
Stakeholder(s)	Directorates, Divisions and decision makers that can affect, be affected by a decision or activity.
Risk Champion	A person that has been given the authority to monitor a particular risk and report to the RM function
Risk Owner	A person with the accountability and authority to manage a risk.
Risk Appetite	Is the amount and type of risk that SBC is willing to pursue or retain.
Risk Tolerance	The acceptable level of risk, defined by the organisation, within which it is willing to operate.
Risk Mitigation	Actions taken to manage the likelihood or impact of risks.
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation.
Risk Identification	The process of finding, recognising and describing risks.
Risk Analysis	The process to comprehend the nature of risk and to determine the level of risk
Risk Evaluation	The process of comparing the results of risk analysis with risk criteria to determine whether the risk and/ or its magnitude is acceptable or tolerable.

Event	Occurrence or change of a particular set of circumstances An event can be one or more occurrences and can have several causes. An event can consist of something not happening. An event can sometimes be referred to as an "incident" or "accident". An event without consequences can also be referred to as a "near miss", "incident", "near hit" or "close call".
Likelihood	The chance of the risk happening.
Impact	Extent to which Slough Borough Council is subject to an event.
Consequence	Outcome of an event affecting Slough Borough Council objectives.
Risk Description	Structured statement of risk usually containing four elements: ***sources, root causes, events and consequences.***
Root Cause	Element which alone or in combination has the intrinsic potential to give rise to risk. A risk source can be tangible or intangible.
Risk Treatment	Process to modify risk which involves accepting, mitigating, transferring, or avoiding the risk.
Control	Measure that is modifying risk. Controls include any process, policy, device, practice, or other actions which modify risk. Controls may not always exert the intended or assumed modifying effect.
Current Risk	The risk, taking into account current controls and their effectiveness.
Monitoring	Continual checking, supervising, observing or determining the status to identify change from the desired or expected performance level.
Risk Reporting	Form of communication intended to inform internal or external stakeholders by providing information regarding the current state of risk and its management.
Risk Management Plan	Scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk. Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities The risk management plan can be applied to a particular product, process and project, and part or whole of the Council.
Risk Aggregation	Combination of a number of risks into one risk to develop a more complete understanding of the overall risk.

4.09 Related Policies and Procedures

Risk Management Board terms of reference (*link*)

ISO 31000: 2018 international risk management standard

Audit & Corporate Governance terms of reference (*link*)