Risk Management Strategy

Contents

Document Control Sheet

Document Title	**WSCC Risk Management Strategy**
Author(s)	T Eves
Document Status	Published

Document Amendment History

Version No.	Date	Amendment Details	Approved By
1.0	1 Mar 17	WSCC RM Strategy published	Dir FSS
2.0	5 Mar 18	WSCC RM Strategy revised	Dir FSS
2.1	24 Apr 18	Para 5.3.3 Action Planning – Amended to capture that the new version risk register now incorporates the action plan	Corp Risk Mgr.
2.2	9 Oct 18	Para 6.2.2 – Addition of guidance for escalating and de-escalating service and directorate risks	Corp Risk Mgr.
2.3	30 Jan 19	App C – Removal of Corporate Business Manager Role	Corp Risk Mgr.
3.0	8 Apr 19	Para 5.6 – reference to ELT viewing key Capital and Transformation risks quarterly	Dir FSS
		Para 6.3.1 – Guidance for inclusion of risk considerations in Decision Reports	Dir FSS
		Fig 3 – Response Guide to support Heat Matrix	Dir FSS
4.0	1 Jul 21	Fig 1 Risk Governance Framework – Inclusion of Scrutiny Committee	Dir FSS
		App D Assessment Criteria – Project/Programme impact area added	Dir FSS
5.0	21 Apr 22	Fig 1 Risk Governance Framework – Inclusion of DLT risk responsibility (pg. 6)	Dir FSS
		App C Roles and Responsibilities – Inclusion of DLT as a key stakeholder (pg. 18)	Dir FSS

Risk Management Policy Statement

This Policy Statement outlines the County Council's commitment to managing risk and should be read in conjunction with the West Sussex County Council Risk Management Strategy (below).

Effective risk management is fundamental to the delivery of the 4 priorities of the County Council: (1) Keeping people safe from vulnerable situations; (2) A sustainable and prosperous economy; (3) Helping people and communities to fulfil their potential; and (4) Making the best use of resources, underpinned by a cross-cutting theme of climate change, as set out in Our Council Plan.

Risk management is an integral part of our corporate governance arrangements and is included within our public quarterly performance and resources reporting to Cabinet.

By ensuring that the risk culture, processes, and frameworks are in place and supported, we can apply robust risk management activity to contribute towards the authority's overall improvement framework. Risk management allows the County Council to be proactive in anticipating and managing problems, rather than reacting when they arise. In addition, it helps inform our integrated business planning, performance management and budgeting processes – which enables the council to take the difficult decisions on where to focus its efforts and limited resources to most effectively deliver the 4 priorities set out in Our Council Plan.

Becky Shaw

Chief Executive
West Sussex County Council

1 Introduction

West Sussex County Council's risk management approach and strategy is based on industry best practice; with alignment to the International Standard in Risk Management (ISO 31000), British Standard Code of Practice for Risk Management (BS ISO 31100) and HM Treasury Management of Risk (The Orange Book); with guidance from Axelos Management of Risk (MoR) and Association of Project Management (APM). A list of definitions and descriptions can be found at Appendix A.

1.1 What Is a Risk?

A risk can be defined as:

"An uncertain event or set of events that, should it occur, will have an effect on the achievement of objectives".

For something to be a risk there must be an element of uncertainty. The effect of uncertainty on an organisation's objectives is therefore a risk. Risk is ever-present and a significant degree of risk-awareness is essential if the Council is to achieve its objectives.

A risk can be either a:

- **Threat** - A risk event that has a negative impact on objectives.
- **Opportunity** - A risk event that has a positive impact on objectives.

Once identified and assessed, they are both managed in the same way.

1.2 What Is Risk Management?

Risk management can be defined as:

*"**Coordinated activities that allows individual risk events and overall risk to be understood and managed proactively, optimizing success by minimising threats and maximising opportunities**".*

Risk management is the process of identifying what might go wrong i.e., what the trigger/source could be, assessing the potential consequences and effects, and deciding how best to minimise the risk of it materialising. If something goes wrong, proactive risk management will significantly improve the chances of keeping the negative impacts to a minimum and/or increase the positive impacts.

Risk management means adopting a planned and systematic approach to the identification, evaluation and management of the risks facing the Council and is a means of minimising the costs, disruption and reputational harm to the Council caused by unexpected events.

Risk management covers the whole spectrum of risk; not just those associated with finance, health and safety or insurance. It also includes risk associated with public image (reputation), the environment, technology, contracts/partnerships, projects etc. A detailed list of risk categories appropriate to the Council can be found at Appendix B.

1.3 Our Approach to Risk Management

To structure and formalise the risk management arrangements across all functions, West Sussex County Council has developed a systematic and logical process of evaluating business risk to ensure it is managed effectively, efficiently, and coherently across the organisation. The Council's adopted approach sets out the methodology for identification, evaluation, and management of risk to ensure the Council can deliver its services efficiently and effectively to the residents of West Sussex.

Council-wide ownership and accountability for managing risk is critical to the success of the organisation. All directorates work to actively anticipate and manage their business risks, embracing opportunities and reducing threats in line with their risk tolerances.

In following 'one' approach, the risk profiles of each function are transparent, and this enables comparisons to be made and risks to be aggregated, empowering a whole organisation.

approach to risk management.

Our approach is to ensure that the discipline of effectively managing risk is integrated throughout the organisation.

Members and senior officers of the council will be primarily focussed on the strategic and business-critical risks that could impact on the achievement of objectives or successful delivery of outcomes. More detailed business operations risks will be the primary concern of services and functions, where managers will be controlling and monitoring their risks and escalating these to a strategic level if they are no longer containable and manageable at a functional level.

Identified risks and risk management actions are managed through the Council's risk registers and should be regularly discussed, reviewed, and updated. Frequent risk reporting takes place across all levels of the organisation.

1.4 Benefits of Risk Management

When implemented and maintained, effective risk management enables the organisation to:

- Prevent the frequency of 'shocks' and unwelcome surprises.
- Focus attention on real and important risks
- Enhance the opportunity to successfully achieve objectives.
- Ensure the effective and efficient use of resources.
- Provide a better service delivery to the customer.
- Internally focus on doing the right things properly
- Develop a proactive, risk aware culture.
- Develop staff and organisational resilience.

1.5 Risk Management Vision

West Sussex County Council's vision for risk management is to ensure that all risks to the achievement of corporate objectives are identified, assessed, and managed effectively. To achieve this, a culture must be embedded and supported where the consideration of risk occurs throughout all levels in the organisation in a consistent way.

1.6 Objectives of Risk Management

West Sussex County Council's objectives of the risk management strategy are to:

- Integrate risk management fully into the culture of the council including its key management processes such as corporate and service planning processes, project and programmes, financial and performance management.
- Ensure there is an effective framework for identifying, assessing, managing, reviewing, reporting, and communicating risks across the council.
- Ensure that Officers, Elected Members, Scrutiny and Audit Committees, and external stakeholders can obtain necessary assurance that the Council is effectively managing and mitigating the risks of not achieving key priorities.
- Maintain clear roles, responsibilities, and reporting lines for risk management.
- Continuously improve risk management throughout the council and proactively communicate the councils risk management approach to staff.
- Ensure risk is managed in accordance with best practice.

1.7 Principles of Risk Management

The key principles to support successful risk management are outlined below:

- All staff are responsible for recognising and actively reducing risk as part of all business processes.
- A consistent risk management approach and language throughout the organisation
- To communicate risk across the Council, through escalation and de-escalation, in a

timely and accurate manner
- Apply the principles of continuous improvement by promoting positive outcomes and learning from mistakes.

1.8 Risk Appetite

Risk appetite is best defined as:

"The amount of risk an organisation is willing to accept, tolerate, or be exposed to at any point in time in order to achieve its objectives" (*HM Treasury Orange Book)

1.8.1 Risk Appetite Statement

The Councils risk appetite statement outlines the principles it will adopt regarding its approach to risk management. The risk appetite has been developed through consideration of the following areas:

- "Our Council Plan"
- Organisation culture
- Realised risks from other local government authorities.

West Sussex County Council accepts that it operates within a high-risk environment and any risk taking must be done in a controlled manner. This means that all risks must be fully understood; with likelihoods and impacts addressed through effective mitigations and communications to reduce the exposure to an acceptable level.
Appetite will vary depending on the activity and risk area. Figure 3 - Summary Risk Profile represents the overall risk appetite for council, not taking into consideration any variables for specific categories of risk. Risks below this appetite will generally be tolerated to avoid assigning a disproportionate amount of resource; however outside of this there may be a need to take mitigating action or escalate/communicate if required.
Although taking risks provides an opportunity to increase the potential for success and/or support innovative activity, the Council will always seek to control risks with at least a 'high' likelihood to:

- Cause significant harm to staff, service users and residents.
- Significantly impact on the environment
- Significantly impact on finances
- Threaten compliance with legal and regulatory requirements.
- Jeopardise the Councils ability to deliver its core purpose.
- Create opportunities for fraud or corruption.

The Council's overall risk appetite (Figure 3 - Summary Risk Profile) and statement will be reviewed annually as part of the Council's risk management strategy review.

1.9 Risk Tolerance Threshold

Risk thresholds (between amber and red) represent the level of exposure which, when exceeded, will trigger immediate actions to reduce it to a more acceptable level. Threshold will often indicate a level where communication or escalation of the risk is required.

1.10 Risk Appetite V Risk Tolerance Threshold

Risk tolerance threshold identifies a limit in which the organisation is not prepared to go to and **must** be dealt with; unlike risk appetite which represents an acceptable level of risk to tolerate.) Risk appetite and risk tolerance threshold help an organisation determine what high, medium, and low risk is (i.e., red, amber, and green on the risk heat map). Defining these levels allow risks to be prioritised and appropriate actions assigned so that the management of identified risks will be proportionate to the decision being made, or the level of impact on service delivery.

Para 5.2.3 (Summary Risk Profile (Heat Map)) illustrates the Council's risk appetite and risk tolerance threshold using a heat map. Both the appetite and threshold of an organisation must be periodically reviewed to ensure risk is

managed and communicated effectively and efficiently, in line with the Council's risk appetite statement.
Risk appetite and tolerance threshold are scalable; what may be considered a high risk in one tier may be a low risk within another tier. The Council's appetite and tolerance threshold is the overall amount of risk judged appropriate to be tolerated or acted upon by the organisation. Lower tiers in the organisation can adapt this to reflect their risk capability, and this will facilitate risk reporting and/or escalation to senior management through exceeding agreed thresholds.

2 Risk Management Framework

The risk management framework incorporates all risk management activity required to embed and operate a consistent, yet flexible, approach across the Council. These activities can be summarised in the following areas:

- **Governance** – Risk Management Strategy
- **Methodology** – Risk Management Process
- **Education** – Risk Management Training and Awareness
- **Assurance** – Internal Audit and Annual Governance Statement

The Council's approach is to ensure risk is managed effectively throughout the organisation; with Members and senior officers focussing on strategic and business critical risks, empowering services to manage and report on detailed operational risks. All risks are recorded in the WSCC format risk register and reviewed, updated, and communicated regularly. The Corporate Risk Manager is responsible for reviewing and updating the framework when necessary, ensuring it continues to add value. Through applying this framework, and Audit support, the Corporate Risk Manager will provide assurance that risk is being effectively managed across the organisation.

3 Risk Governance Framework

The Risk Governance Framework (Figure 1 - Risk Governance Framework) sets out the various groups, teams, and boards where business risk management activity and intelligence are discussed and reported.
The reporting arrangements span through all levels of the organisation, including the senior officers and Members, to ensure risk information can be escalated, de-escalated, and used as an effective tool to aid decision making. The framework interacts across all directorates and in future will span further to include our partner organisations and commissioned services.

The provision of good risk intelligence promotes discussion, encourages challenge, and enables the organisation to consider risks and opportunities as an integrated element of the day-to-day management operation of the business.

Directors should maintain a record of key operational risks within their service area relating to service change, projects, and significant procurement. Progress in managing these risks should be monitored on a regular basis and discussed with the relevant Cabinet Member.

Internal Audit will conduct a periodic review of the Council's risk management arrangements to provide independent assurance as to their effectiveness. Through the course of the year Internal Audit will also:

- Identify and report weaknesses in the controls established by management to manage/ monitor risks.
- Provide advice on the design/operation of the controls established by management to manage/monitor risk.

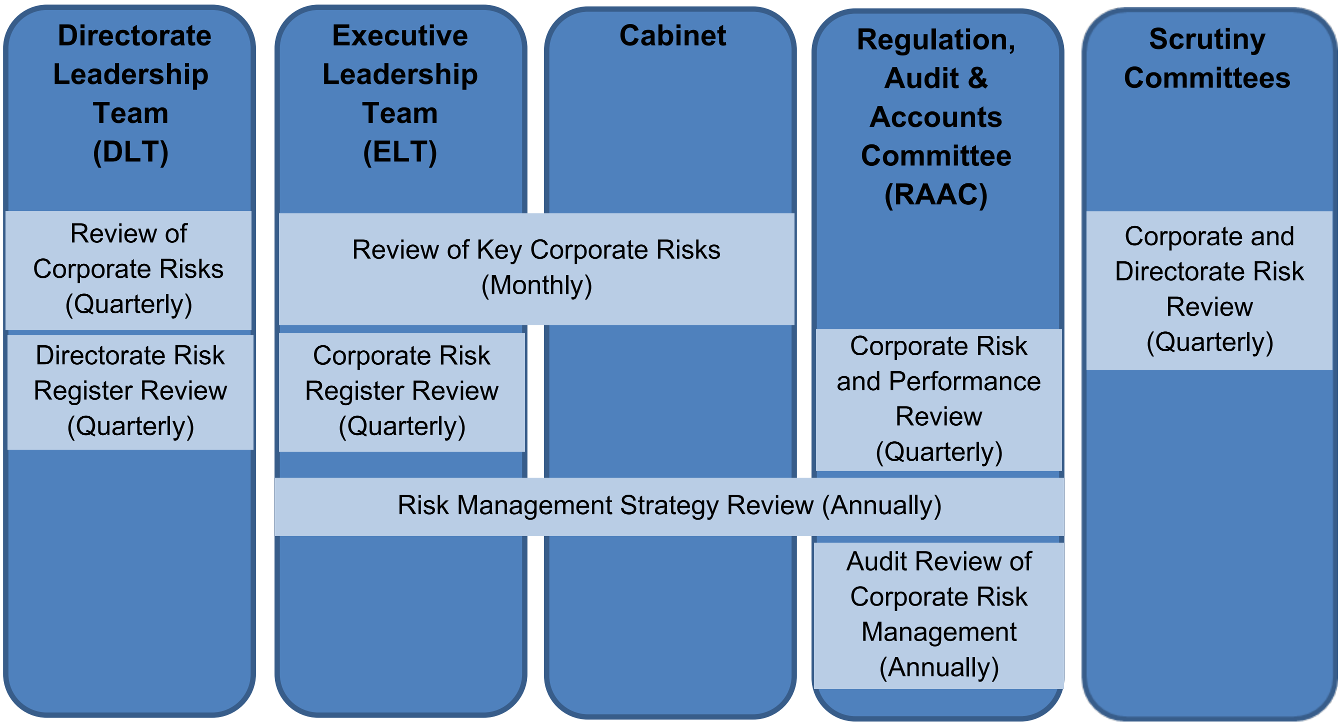

Figure 1 - Risk Governance Framework

4 Roles and Responsibilities

All Members, senior leaders and employees have a role to play in ensuring that risk is effectively managed across the organisation. The risk management strategy is fully endorsed and supported by the Chief Executive and the Leader of the Council, who set the organisational tone for risk management and champion the benefits throughout the Council.

To successfully embed the management of risk into the Council's business as usual operations, it is vital to formalise the roles and responsibilities of individuals and groups involved throughout the risk management process. Appendix C outlines the key responsibilities for each stakeholder (group and individual).

5 Risk Management Model

The risk management process Figure 2 - Risk Management Model (*adapted from HM Treasury Orange Book) is a series of logical steps which are carried out in sequence to progress through each stage of managing a risk. The process is cyclical, and it is often necessary to revisit earlier steps and carry them out again to ensure you have a complete picture of the risks to the activity/outcome you are assessing.

There are many variations of the 'Risk Management Process,' with WSCC aligning itself to the process adopted by HM Treasury (Orange Book). This model focusses less on rigidity of process but encourages awareness of organisational and risk context and how key inputs influence outputs.

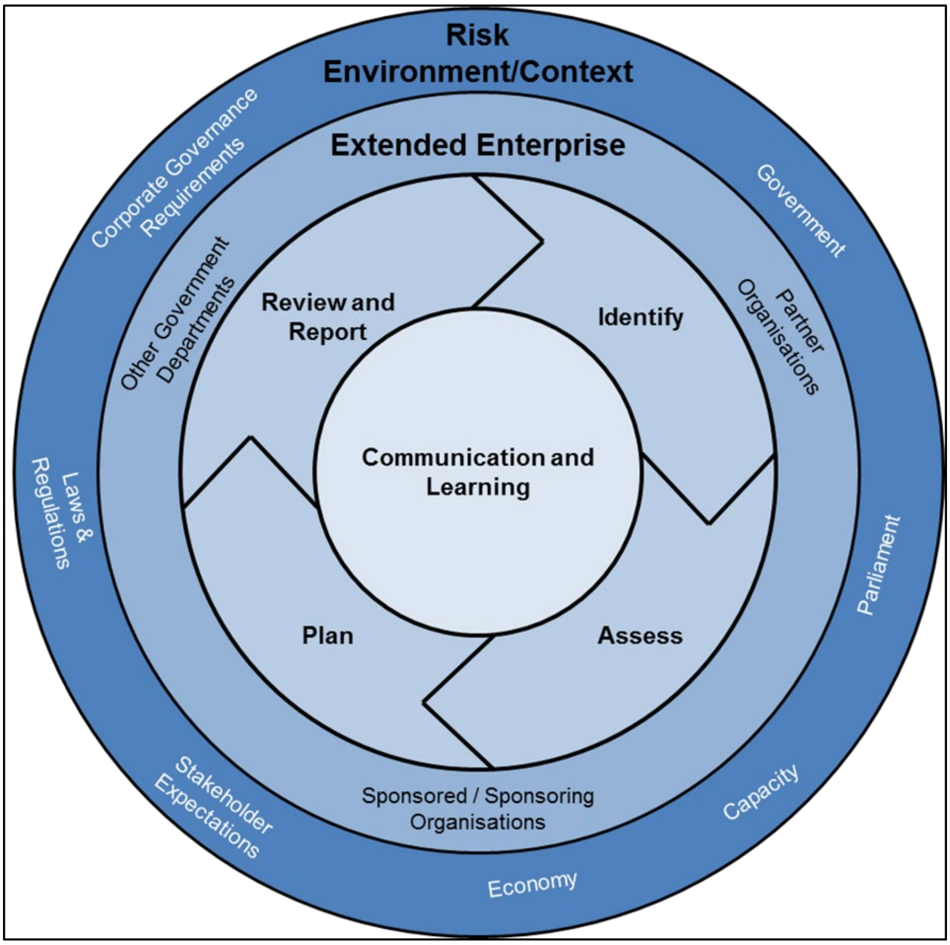

Figure 2 - Risk Management Model (*adapted from HM Treasury Orange Book)

5.1 Identify Risks

The risk identification stage provides a structured approach to inform how objectives may be affected by risk. This should be conducted iteratively; and must be sufficiently detailed, precise, and consistent to generate and record a list of comprehensive risks. It is important to establish the context around which you want to identify and assess risks i.e., an activity, objective, or outcome.

5.2 Assess Risks

Risk assessment determines the significance of a risk by understanding two factors; potential <u>impact</u> of the risk if it were to occur, and the <u>likelihood</u> of the risk occurring. Risk analysis may be undertaken with varying degrees of detail depending upon the risk, the purpose of the analysis, and the information, data, and resources available.

To ensure consistency of assessment of the probability and impact, a defined set of criteria has been produced. This criterion allows all risk to be measured against five levels of severity across 9 impact areas:

- Objectives
- Service
- Projects/Programmes
- Infrastructure
- Environment
- Finance (including claims)
- Safety
- Human Resources
- Statutory/Legal
- Reputation

The Council's directorate and corporate risk assessment criteria can be found at Appendix D.

5.2.2 Types of Risk Score

Using the risk assessment criteria, three different types of risk score can be assessed to fully understand and monitor the true nature and size of the risk: initial, target and current.

- **Initial Risk Score (pre-mitigation i.e., inherent risk)** - This is an assessment of the impact and likelihood of a risk based on its **current** status (worst case scenario).
- **Target Risk Score (post-mitigation)** - This is the desired impact and likelihood levels based on the amount of exposure the organisation, directorate or service is comfortable to tolerate (**after** additional controls have been taken into account).
- **Current Risk Score (risk score at review i.e., residual risk)** - This assessment illustrates whether the target score is on track to be achieved.

5.2.3 Summary Risk Profile (Heat map)

A heat map (Figure 3 - Summary Risk Profile) is a simple, visual tool that can be used in reporting to increase the visibility of risks and is a graphical representation of the information on the risk register; determined during analysis and scoring. A risk profile shows all key risks as one picture, so that managers can gain an overall appreciation of the total exposure to risk. The Council's corporate risk profile (below) shows the risk threshold and appetite which will immediately inform owners if mitigating action is required. The summary risk profile must be reviewed at least annually to reflect any changes in the Council's risk appetite statement and tolerable thresholds.

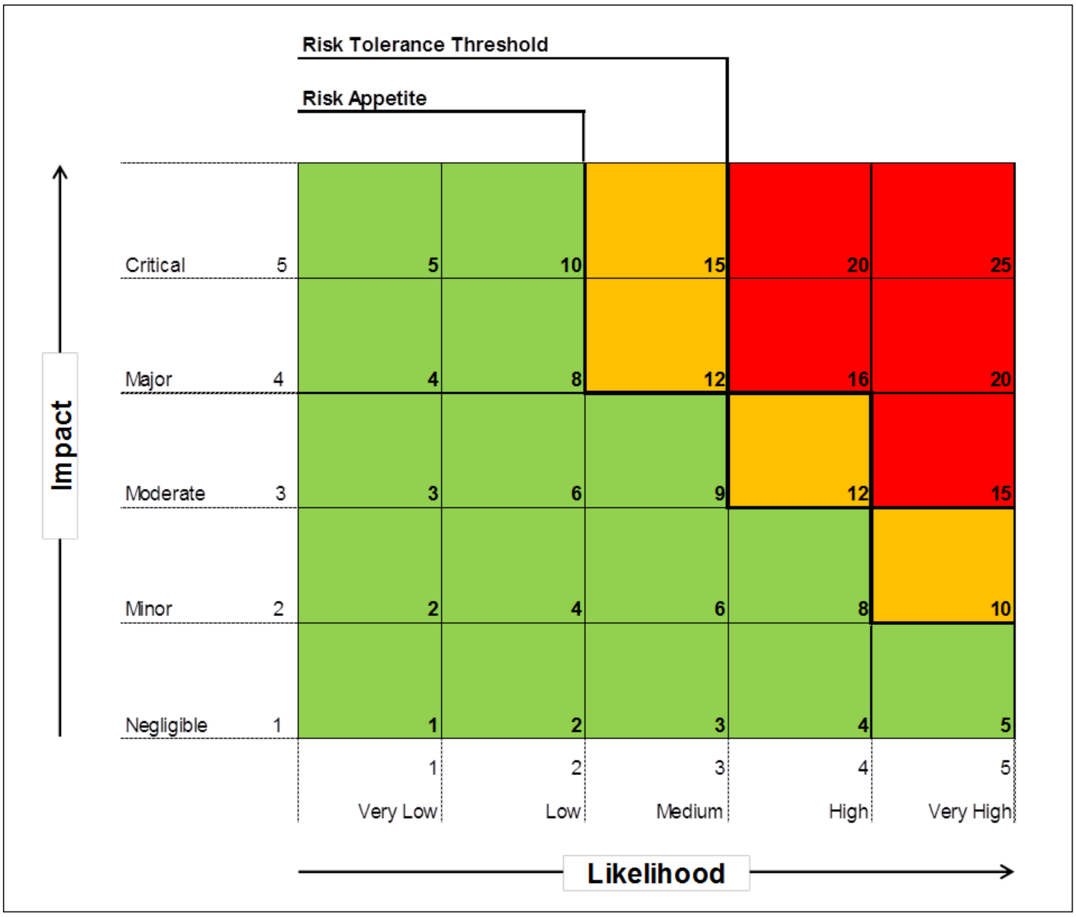

Figure 3 - Summary Risk Profile

Risk Assessment Rating	Green	Amber	Red
Action Guide	Acceptable level of risk managed by routine controls at appropriate level.	Possible unacceptable level of risk exposure, requiring constant active monitoring and controls at appropriate level.	Unacceptable level of risk exposure requiring immediate corrective action to be taken at appropriate level.
Summary	Within risk appetite. Accept risk or manage/monitor.	Outside of risk appetite, but within tolerance threshold. May be tolerable but could look to reduce to within appetite.	Outside of risk appetite and outside of tolerance threshold. Requires immediate action to reduce to within tolerance threshold or risk appetite.

Figure 4 - Response Guide

5.3 Plan Responses

Once it has been determined that a risk requires additional action, a decision must be made on the best strategy that will enable the achievement of the target score.

5.3.1 Risk Response Strategies

Risk responses can be grouped into strategies as shown below in Table 1 - Risk Response Strategies

Risk Response Strategy	Examples
Tolerate Accept the risk / do nothing	• Cost of action disproportionate to the benefits gained. • Limited ability to treat risk. • Contingency plan is produced. • Risk is within appetite or threshold and is tolerable
Treat Action taken to reduce impact or likelihood, or both	• Separation of duty. No one person can act without consent of another (remove single point of failure). • Produce contingency plan to reduce impact level. • Wearing of protective clothing or training given
Transfer Reduce exposure of risk by transferring or sharing the risk	• Taking out insurance • Transfer to third party i.e., sub-contractor Not all risks are fully transferred i.e., some risk to the Council may remain i.e., reputational

Risk Response Strategy	Examples
Terminate Stopping the activities that gives rise to the risk	• Replace activity giving rise to the risk with an alternative activity. This strategy has limited use in the Council as termination of an activity may result in lack of service to the customer
Take the Opportunity Exploit the opportunity to deliver positive benefits / outcomes	• Undertake an action or manage a set of circumstances to increase likelihood of realising a positive outcome.

Table 1 - Risk Response Strategies

5.3.2 Risk Register

The risk register is owned by the manager for that organisational area and is a repository for all the risks that may have an impact on the organisational objectives or activity.

5.3.3 Action Planning (Risk Treatment Plans)

Once the risk has been assessed, prioritised and response strategy determined; an action plan (risk treatment plan) is determined and should consider the following:

- **Response priorities** – understand the impact on other activities and availability of resources.

- **Assign action owners** – to ensures individual or multiple risk responses are implemented.

- **Prepare a schedule** – timeline to implement actions (agreed with action owner)

Part of the risk register, the action plan specifies the response strategy controls, assigning action owners to ensure the responses are managed, monitored, and reported.

5.4 Review and Report

The management of risk must be reviewed and reported on for two reasons:

- To monitor whether the risk profile is changing.
- To gain assurance that risk management is effective.
- To identify when further action is necessary.

The risk owner should establish the frequency of the review and ensure that any significant changes to the risk are reported or escalated to the appropriate levels.

The purpose of risk reporting is to present risk information in a consistent and timely manner, with the frequency and format to be determined by management needs, risk severity and organisational objectives.

The primary function of reporting on risk is to:

- Inform decision making.
- Enable further analysis.
- Provide oversight and opportunity to challenge.

5.5 Communication and Learning

Communication and consultation should begin the instant the risk management process is entered into; with proportionate engagement with stakeholders (internal and external) paramount to successful data capture.

It is important to ensure that transferable lessons are learned and communicated to those who may benefit from them. This positive lesson will be captured and communicated across the Council for others, who encounter the same or similar risk, to have the benefit of this knowledge.

5.6 Project, Programme and Portfolio Risks

Project and programme risks are managed in the same way as other risks in the Council but there are slight differences in the approach. Risk registers or logs will still be maintained for risks to programmes or projects but will be appropriate to support the delivery of the work being conducted.

Any project, programme or portfolio should align itself to the WSCC Risk Management Strategy; however, it should have its own risk management guidelines, roles and responsibilities, and escalation/reporting protocols to support the successful delivery. Individual project/programme risks should not be captured in a directorate or the corporate risk register, however, progress and issues related to cross-department projects/ programmes should be communicated to ELT and stakeholder groups when necessary.

Capital risks will continue to report to their respective boards; however, a summary of key risks will be viewed quarterly by ELT.

6 Communication

6.1 Communication Levels

The Council's approach to risk management relies upon effective and consistent communication across all levels in the organisation. It is important to understand the communicative relationship between these levels to accelerate the forwarding or transferring of information.

6.2 Escalation and De-escalation

A risk can be moved to a higher level in the organisation (escalated) for the following reasons:

- The risk becomes unmanageable.
- The risk is outside of the appetite boundaries.
- The risk remains very high after control measures have been implemented.
- The risk impacts on more than one Directorate/project or programme/department
- The risk is directly related to an organisational objective.

A risk can be moved to a lower level in the organisation (de-escalated) for the following reasons:

- The risk will only affect one Directorate/project or programme/functional area and is better controlled locally.
- The risk rating has decreased significantly or is not considered to be critical to the achievement of a strategic objective.
- The risk can be controlled and managed at a lower level.

It is important to consider the risk appetite of the level the risk is being de-escalated to as this could significantly impact how effectively it is managed (i.e., capability, resource).

Before a risk can be escalated or de-escalated, it must be clear who the risk owner is. If a new risk owner is identified, they must agree to this transfer of ownership and be contacted for a handover. At this point the risk should be re-evaluated to take into consideration the appetite of the new owner/level in the organisation.

Once a risk has been escalated or de-escalated it is removed from the preceding risk register as a risk should only be present on one risk register. There may be exceptions where a risk is required to be visible on more than one risk register; if this occurs, advice of the Corporate Risk Manager should be sought.

6.2.1 Escalation and De-escalation of Corporate Risks

On a quarterly basis the ELT will review the corporate risk register and discuss inclusions and deletions of risks proposed. Should a risk require urgent discussion and possible inclusion on the corporate risk register outside of this meeting, it is to be highlighted to the Corporate Risk Manager in the first instance. The Corporate Risk Manager will review the risk and facilitate a discussion with the Director of Finance and Support Services. If accepted, this will be presented to ELT for consideration for inclusion on the corporate risk register.

6.2.2 Escalation and De-escalation of Directorate Risks

The escalation of risks to a directorate risk register should take place at the respective management team meeting. It is at the same meeting that risks can be removed from the directorate risk register; de-escalated to be managed at a service level or removed completely.

The Corporate Risk Manager is frequently invited to attend to support risk capture and articulation; and to encourage effective conversation.

In addition, discussions regarding the escalation of an existing directorate risk to the corporate risk register should take place at this management team meeting. Should escalation be required, the details in para 6.2.1 are to be followed. The Corporate Risk Manager should be invited to attend management team meetings to support risk discussions, provide guidance and support, and advise on escalation.

6.3 Reporting

Risk reporting is the set of activities that ensures information on risk is captured, documented, communicated, and understood in a consistent way across the organisation. For this to be achieved, it is advised to create an opportunity at the management team meeting to collectively discuss key risks (not escalation initially). Risk reporting is used to provide visibility and understanding of risks to:

- Inform decision making.
- Provide confidence to stakeholders.
- Enable further understanding and analysis.

An additional supporting document to the risk register can be produced in brief (or verbally delivered), to provide a clear representation of the current risk status. Suggested content of this is as follows:

- Highlighting key risks to the service/directorate/organisation
- What is being done to mitigate these key risks?
- Emerging or new risks

6.3.1 Decision Reports

To ensure the assessments of propositions are effectively conducted, it is essential that all decision reports specify the risks associated with courses of action, including recommended mitigating actions. Tangible data specifying the impact/exposure should be included where possible. Further guidance is included within the decision report template.

7 Guidance, Education and Training

Knowledge of how to manage risk is essential in embedding and maintaining an effective risk management system. The Corporate Risk Manager is responsible for developing workforce risk management capability across the organisation through the provision of guidance, education, training, and support.

The risk management strategy and supporting guidance are reviewed and improved on a regular basis to ensure they meet the needs of the Council. Direct learning and e-learning packages of training have been developed and will be available and accessible to all Council staff. All learning needs analysis and subsequent training is developed and monitored in accordance with the Council's Learning and Development Policy.

A risk management intranet page has been developed so all documents to support the implementation of risk management can be centrally located. A blank risk register is available to download for editing purposes.

Specific training is available on request, on the following areas:

- Risk Management Process
- Risk register
- Scoring and grading
- Practical use of the register
- WSCC Risk Management Strategy

8 Quality Assurance

To ensure that the Council's risk management framework remains fit for purpose we continually review and update our risk management methodology. By embracing innovative ideas and changes to industry best practice, we can maintain a flexible framework to adapt to our changing operational environment and economic conditions.

8.1 Internal Audit

Internal Audit will conduct a periodic review of the Council's risk management arrangements to provide independent assurance as to their effectiveness.

Through the course of the year Internal Audit will also:

- Identify and report weaknesses in the controls established by management to manage/monitor risks.
- Provide advice on the design/operation of the controls established by management to manage/monitor risk.

Internal Audit and RAAC will review the corporate risk register on an annual basis to inform the Internal Audit planning process.

8.2 Risk Maturity Assessments

The need for an assessment is still under consideration.

8.3 Annual Review

The risk management strategy, guidance and training materials are reviewed at least annually to ensure they continue to meet the needs of the organisation and incorporate the very latest industry best practice.

Appendix A Glossary of Terms

Term	Definition
Assurance	An evaluated opinion, based on evidence gained from review, on the organisation's governance, risk management and internal control framework.
Action Owner	Ensuring individual or multiple risk responses are implemented, with updates on developments reported back to the Risk Owner. The Risk Owner delegates responsibility to the Action Owner, but still maintains overall accountability for the risk.
Cause	The reason why the risk could happen; internal or external.
Consequence	Effects arising from the risk event measured through impacts e.g., finances, reputation.
Contingency Planning	Process of identifying and planning a secondary response should the planned outcome be ineffective or doesn't reduce the risk to a tolerable level. Often used for potentially catastrophic risks.
Current Risk	Illustrates whether the target score is on track to be achieved taking into account the progress of the mitigating controls (existing and additional) and the current risk climate/context.
Emerging Risk	New or evolving risks that are difficult to characterise or assess now due to limited information being available, and/or lack of prior experience of the specific type of risk.
Event	Incidents or occurrences that arise from the cause.
Horizon Scanning	Systematic activity designed to identify, as early as possible, indicators of changes in risk.
Impact	Estimate of the potential severity of the effect on objectives, should the risk occur i.e., financial, reputational, safety.
Initial Risk	An assessment of the impact and likelihood of a risk based on its current status whether there are no mitigating controls or actions in place, or the existing controls or actions do not work as intended. This assessment determines the 'worst case scenario.'
Likelihood	Estimate of the probability of a risk occurring.
Proximity	Identifying a point in time when the risk is likely to happen.
Risk	An uncertain event or set of events that, should it occur, will have an effect on the achievement of objectives.
Risk Assessment	The evaluation of risk regarding the impact if the risk is realised and the likelihood of the risk being realised.
Risk Assessment	The evaluation of risk regarding the impact if the risk is realised and the likelihood of the risk being realised.
Risk Categories	Defined groupings of risk based on the Council's services and activities.
Risk Description	A description of the cause, event, and consequence of the risk to enable likelihood and impact to be assessed, and effective controls to be determined.
Risk Management	Coordinated activities that allow individual risk events and overall risk to be understood and managed proactively, optimizing success by minimizing threats and maximizing opportunities.

Term	Definition
Risk Owner	The individual who is accountable for monitoring the risk and ensuring mitigating actions are being carried out.
Risk Register	A repository for capturing and recording risks and associated information.
Risk Actions/Mitigations	An activity or measure that is expected to reduce the impact or likelihood of a risk event.
Secondary Risk	An additional risk that may materialise as a direct result of implementing a risk response
Target Risk	The desired impact and likelihood levels based on the amount of exposure the organisation, directorate or service is comfortable to tolerate It requires the assessment of the impact and likelihood of a risk after additional mitigating controls have been taken into account.

(*adapted from HM Treasury Orange Book)

Appendix B Risk Categories

Categories	Description
Political	**Global, European, national, sub-regional or local politics**. Consider election cycles, policy direction, political reorganisations, political relationships and styles, activism, war, and terrorism.
Governance	**Corporate governance and decision-making arrangements**. Consider the constitution, codes of conduct, leadership, culture, and behaviours, checks and balances, and member-officer relations.
Managerial/ Professional	**Managerial and professional needs & situation**. Consider recruitment and retention, succession planning, management style, management systems (e.g., project management, performance management), staffing, reliance on interims/agency staff/consultants, morale, capacity, skills, professional judgement, absence management, grievance and disciplinary policies, and employee relations.
Legislative/Regulatory	**Current and future legislative & regulatory arrangements**. Consider new and pipeline legislation and the Council's audit and regulatory environment. May also relate to the Council's own legal and regulatory powers.
Competitive	**Current and future market situation and the Council's competitors**. Consider exposure to the market, competitiveness/value for money of services, spotlight seeking (for pathfinders, awards, etc.) and competition with nearby or benchmark organisations.
Reputation	**Council's reputation with government, partners, the media, and the public.** Consider loss resulting from damages to the Council's reputation; increased operating, capital, or regulatory costs; consequences to an adverse or potentially criminal event even if the Council is not found guilty.
Economic	**Current and future economic situation**. Consider global, national, and local economy (e.g., economic cycles, the economic base, employment and earnings patterns, migration, and inflow patterns).
Social	**Current and future social situations and decisions**. Consider global, national, and local demographics and social trends (like age profile, ethnic profile, health trends, crime trends, skills base and educational provision and attainment). Also consider impact of adopting/implementing a particular service or product.
Environmental	**Potential harm to the environment caused by the Council or partners activities, current infrastructure, or controls**. Consider the physical environment (e.g., like waste, drainage and flooding, disease, pollution, contamination, seismic activity, air quality, water quality, energy use and efficiency, noise).
Customer/ Citizen	**Customer expectations and satisfaction**. Consider the need to meet changing needs and expectations of the public and employees. It also covers complaints and litigation culture.
Partnership/ Contractual/ Supplier	**Council's partnerships, contracts, and supply chain**. Consider procurement, contract and relationship management, governance, funding, skills, quality, and effectiveness.

Categories	Description
Technological	**Threats to assets and processes to maintain effective business operations**. Consider strategy, innovation, obsolescence, the nature of systems, support, maintenance, access, security, data protection and reporting.
Financial	**Financial situation, constraints, processes, and systems**. Consider the adequacy of funding, gearing, financial planning, financial delegations, budgetary control, monitoring and reporting, commitments, cash and treasury management, taxation, pension funds, insurance.
Legal	**Potential for losses due to legal or regulatory action**. Consider compliance with legislation and its legal advice and support.
Physical	**Potential of harm due to inadequate/unsuitable products or associated management**. Consider the asset base (i.e., buildings, vehicles, drainage, highways, bridges, plant, and equipment) and its health & safety and security systems.

Appendix C Roles and Responsibilities

Role	Responsibility
Cabinet – Leader and individual Cabinet Members	• Assurance and performance management of Council Plan and budget (Revenue and capital), seeking assurance that corporate risk is effectively managed
Chief Executive	• Approve the Risk Management Strategy • Accountable to the County Council for the effectiveness of corporate risk management
Regulations, Audit & Accounts Committee (RAAC)	• To monitor the effectiveness of risk management arrangements, including annually agreeing the Council's risk approach as detailed in the Risk Management Strategy
Elected Members and Scrutiny Committees	• To undertake the scrutiny of proposed decisions and the performance of the Council's services against the agreed outcomes, objectives, and measures; including the scrutiny of how effectively relevant corporate and service risks are managed
Executive Leadership Team (ELT)	• Manage the Corporate Risk Register • Ensure all Directorate risks and action plans are up to date. • Provide assurance of compliance with the risk management strategy • Periodically review and update the Council's risk appetite
Directorate Leadership Team (DLT) - also referred to as either Senior Management Team (SMT) or Senior Leadership Team (SLT)	• Ensure corporate risks in their respective business area are kept up-to-date and record the current risk exposure. • Ensure adherence with the Risk Management Strategy • Take ownership of risks within their directorate and ensure risk registers are regularly discussed, reviewed, updated, and escalated as appropriate. • Promote the benefits of effective risk management
Director of Finance and Support Services	• Overall management of all arrangements for an effective risk management function • Approver for escalation and de-escalation of risks to/from the corporate risk register (outside of ELT schedule)

Role	Responsibility
Director of Law and Assurance	• Assurance of the Councils risk management function in accordance with industry best practice
Service Managers	• Manage risks effectively in their service area, in accordance with the risk management framework. • Where necessary escalate risks; and accept de-escalated risks. • Ensure their staff have an understanding and training on risk management. • Promote the benefits of risk management across their service and communicate the corporate approach to managing risk
Employees	• Manage risk as part of their job and report risks to their managers • Develop understanding of risk management across the Council • Maintain awareness of risks, their impact, and costs, and manage these through the adopted risk management process
Corporate Risk Manager	• Manage the administration of risk management and review and develop the strategy and process in accordance with best practice • Provide advice and support to the Executive and Directorate Leadership Teams, and Service Managers on the identification, analysis, prioritisation, and progress of risk • Develop guidance, tools, and training to support the business to manage risk effectively • Report on the identification and progress of strategic risks to the Regulations, Audit & Accounts Committee (RAAC)
Internal Audit	• To provide reasonable assurance over the organisation's framework of risk management. • Through their risk-based approach contribute to the wider assurances that controls to mitigate key risks are operating effectively.

Appendix D Risk Assessment Criteria

Risk Likelihood Criteria

Likelihood	Score	Frequency	Description
Very High	5	Common occurrence at WSCC or other local authorities.	There is strong evidence (or belief) to suggest that the risk will occur during the timescale concerned.
High	4	Has occurred at WSCC or other local authority many times.	There is significant evidence (or belief) to suggest that the risk will occur during the timescale concerned.
Medium	3	Has occurred at WSCC or other local authority several times.	There is some evidence (or belief) to suggest that the risk may occur during the timescale concerned.
Low	2	Has occurred at WSCC or other local authority on a small number of occasions.	There is little evidence (or belief) to suggest that the risk may occur during the timescale concerned.
Very Low	1	Has occurred at WSCC or other local authority once/never.	There is no evidence (or belief) to suggest that the risk may occur during the timescale concerned.

Risk Impact Criteria

Domain	Impact Area	5 Critical	4 Major	3 Moderate	2 Minor	1 Negligible
Purpose	**Objectives**	Critical failure or delay in delivering key Council objectives and national policies.	Major failure or delay in delivering Council objectives and national policies.	Moderate failure or delay in delivering Council objectives and national policies.	Minor failure or delay in delivering Council objectives and national policies.	Insignificant failure or delay in delivering Council objectives and national policies.
	Service	Loss of key service >14days.	Loss of key service 7-14 days.	Loss of key service for <7 days.	Minor service interruptions.	Insignificant service interruptions.
	Projects/ Programmes	Associated service loss for a significant period. Project(s) on hold or terminated. Failure to meet project acceptance criteria.	Significant disruption to any associated service activity. Significant impact on project(s) acceptance criteria.	Disruption to any associated service activity. Impact on project(s) acceptance criteria.	Minor disruption to any associated service activity. Minor impact on project(s) acceptance criteria.	Failure to meet a minor acceptance criterion but does not disrupt project(s) or any service activity.
Property	**Infrastructure**	Long term infrastructure damage	Medium term infrastructure damage	Some medium-term infrastructure damage	Minor, short term infrastructure damage	Negligible infrastructure damage
	Environment	Long term environmental damage	Medium term environmental damage	Some medium-term environmental damage	Minor, short term environmental damage	Negligible environmental damage
Pounds	**Financial (inc. claims and revenue)**	Losses >£1m Loss of more than 35% of service budget >30% increase in project/programme budget (not including allocated/planned contingencies)	Losses £501k to £1m Loss of 20-35% of service budget 15-30% increase in project/programme budget (not including allocated/planned contingencies)	Losses £151k to £500k Loss of 10-20% of service budget 10-15% increase in project/programme budget (not including allocated/planned contingencies)	Losses £51k to £150k Loss of 5-10% of service budget 5-10% increase in project/programme budget (not including allocated/planned contingencies)	Losses < £50k Loss of up 5% of service budget <5% increase in project/programme budget (not including allocated/planned contingencies)

Domain	Impact Area	5 Critical	4 Major	3 Moderate	2 Minor	1 Negligible
People	**Safety**	Incident leading to death. Multiple permanent injuries or irreversible health effects.	Major injury leading to long-term incapacity/disability. Requiring time off work for >14 days.	Moderate injury requiring professional intervention. Requiring time off work for 4-14 days.	Minor injury or illness, requiring minor intervention. Requiring time off work for <4 days	Minimal injury requiring no/minimal intervention or treatment. No time off work.
	HR	Non-delivery of key objective/service due to lack of staff. Ongoing unsafe staffing levels or competence. Loss of several key staff. No staff attending mandatory training on an ongoing basis.	Uncertain delivery of key objective/service due to lack of staff. Unsafe staffing level or competence (>5 days). Loss of key staff. Very low staff morale. No staff attending mandatory/ key training.	Late delivery of key objective/ service due to lack of staff. Unsafe staffing level or competence (>1 day). Low staff morale. Poor staff attendance for mandatory/key training.	Low staffing level that reduces the service quality.	Short-term low staffing level that temporarily reduces service quality (< 1 day).
Profile	**Statutory/ Legal**	Multiple breeches in statutory duty. Serious findings by audit/inspection; serious court enforcement or prosecution.	Major findings by audit/inspection. Court enforcement or prosecution.	Significant findings by audit/inspection. Minor court enforcement or prosecution.	Minor findings by audit/inspection. Minor court enforcement or prosecution.	Insignificant findings by audit/inspection.
	Reputational	Prolonged adverse national media coverage. Long term reduction in stakeholder confidence. Intervention by commissioners.	Some adverse national media or prolonged local media coverage. Medium term reduction in stakeholder confidence.	Some adverse local media coverage. Short term reduction in stakeholder confidence.	Some adverse local media coverage. Element of stakeholder concern.	Local interest/rumours. Potential for stakeholder concern.