Annex 1

Risk Management Strategy

2021

SURREY COUNTY COUNCIL

Contents

1 Introduction

A risk is defined as an uncertain event which, should it occur, will influence the achievement of objectives. This Risk Management Strategy outlines the approach used by Surrey County Council in managing risk. A framework is detailed showing the process for undertaking risk identification, assessment, treatment, monitoring and reporting.

By operating a robust risk management process the following benefits can be derived:

- **Strengthen accountability** – through clear and robust risk governance including risk roles and responsibilities, risk ownership, risk monitoring, escalation of risks and oversight of the risk management process
- **Make best use of resources** – through relevant and proportionate treatment of risks, taking account of the level of risk
- **Build stakeholder trust** – by demonstrating that significant risks are consistently identified, assessed, managed, and monitored at the appropriate level across Surrey County Council
- **Avoid surprises** – providing a consistent approach to identify, understand, and assess risks
- **Give confidence** – that appropriate actions are being taken to manage risks in a timely manner
- **Make informed decisions** – with reliable information on risks

The aim of Surrey County Council is to continuously improve its approach to risk management, prompted by new ideas and best practice. In particular, this strategy has drawn on guidance from:

The Orange Book, Management of Risk: Principles and Concepts *(HM Government, 2020)*

Fundamentals of Risk Management (*The Institute of Risk Management 2018)*

Management of Risk: *Guide for Practitioners (OGC, 2010)*

This Risk Management Strategy will be reviewed annually by the Risk Manager and brought to the Audit and Governance Committee for review and approval.

2 Roles & Responsibilities

A number of key roles have been defined in supporting this risk management process:

Risk Owner: To manage any risks assigned and to provide up-to-date, accurate information about the risk

- *Work to develop suitable controls, actions and target completion dates*
- *Review risk including progress against plan, effectiveness of actions taken and any other factors that have impacted the risk*
- *Provide up-to date-risk information including any significant changes to risk levels and progress against treatment plans, to support timely and accurate risk reporting*

Directorate Lead / Service Lead: To coordinate the risk management process across their respective Directorate / Service

- *Manage the implementation of the risk management process across the Directorate or Service*
- *Monitor risk with Risk Owners and ensure the Directorate/Service risk register is updated*
- *Escalate or downgrade risks as appropriate*

Corporate Leadership Team: To support the effective implementation of risk management in the organisation

- *Promote a risk management culture*
- *Review the organisations top risks and ensure suitable mitigations are in place*

Audit & Governance Committee: To ensure that there are adequate risk management processes and activities taking place to protect the viability of the organisation

- *Approve the Risk Management Strategy*
- *Review the top risks for the organisation*
- *Consider recommendations for improvements to the overall management of risk*

Risk Manager: To ensure risk management is consistently applied across the Council

- *Manage the implementation of the Risk Management Strategy (and update as needed)*
- *Provide support and guidance on risk management to the organisation*
- *Maintain the Corporate Risk Register and ensure Directorate/Service risk registers are maintained*

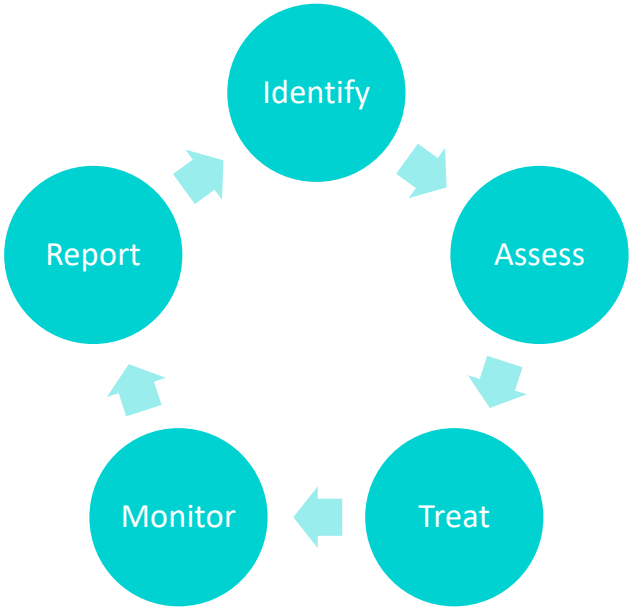
3 Risk Management Approach

(i) The Risk Process

In order to manage risk, Surrey County Council needs to first know what risks it faces and then how best to deal with them. To achieve this, a risk process is used (as shown in Fig 1.) The process highlights each of the risk stages, namely: identify, assess, treat, monitor and report.

More information on the activities undertaken at each stage of the risk process are detailed in the forthcoming chapters of this document.

Fig 1 - The Risk Management Process

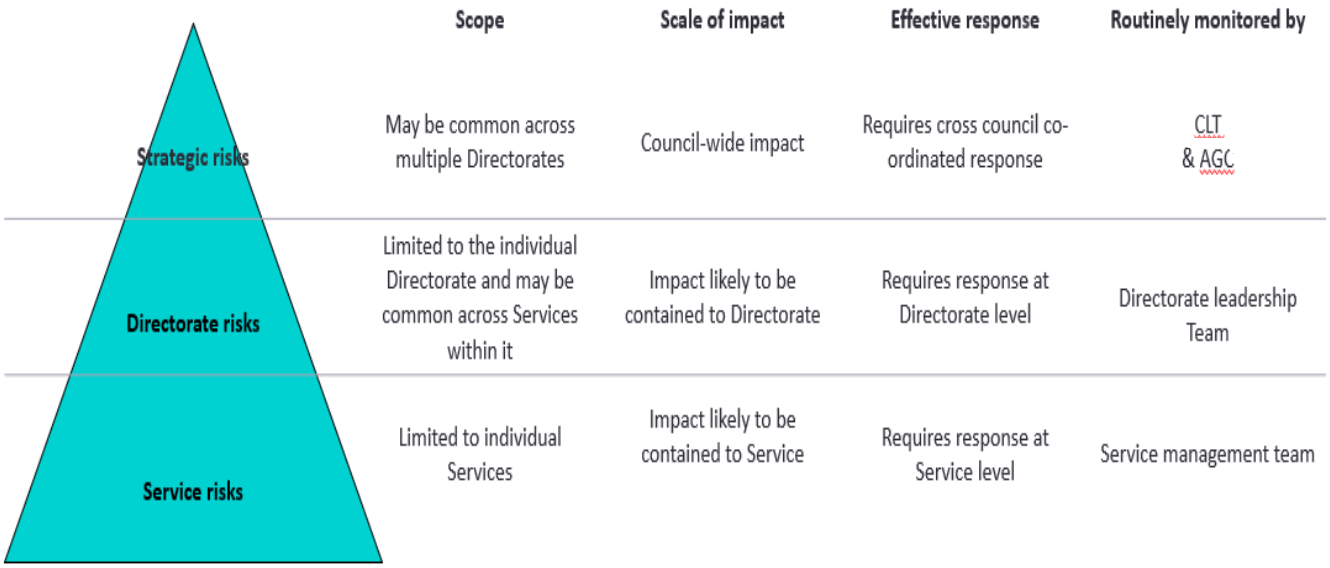


(ii) Risk Hierarchy

The primary method for prioritising risks in Surrey County Council is classifying the risk as either a **Strategic (Corporate), Directorate** or **Service** level risk. Hence, this hierarchy informs the level in the organisation at which the risk is routinely managed and monitored.

Typically, the level of a risk will depend on the scope, scale of potential impact and nature of the response required to manage the risk. Examples of the types of attributes commonly associated with the 3 hierarchy levels are shown in Fig 2. Regardless of level assigned, any risk may be escalated for review or intervention if required (by the Risk Owner or via the Risk Manager).

Fig 2 – The Risk Hierarchy



Once the hierarchy is decided it is then possible to assign the risk to the correct risk register.

(iii) Risk Registers

Risk registers run alongside the risk management process and are used as the key tool to capture risk information in a structured and consistent way. The following risk registers are used within Surrey County Council:

Type of Risk	Risk Register Used	Owner of Risk Register
Strategic	Corporate Risk Register	Risk Manager
Directorate	Specific Risk Register for that Directorate	Head of Directorate
Service	Specific Risk Register for that Service	Head of Service

The format of the risk register used in Surrey County Council is shown in Annex A along with an explanation of the information required to populate. The focus of the risk register is to detail what the cause(s) and effect(s) of the risk are, the likelihood and impact, and the controls and mitigations. To help understand what risk information needs to be captured at each stage of the risk process a summary is shown at the end of each of the following Chapters - see *'Risk Register updated'.*

The frequency of reviewing and updating risk registers will depend on a number of factors such as the threat to the organisations objectives and the volatility of the risk i.e. the rate of change. It is recommended that risks are reviewed at least monthly (depending on the nature of the risk) **but as a minimum all risk should be reviewed at least quarterly.**

4 Risk Identification

Risk identification is the first step of the risk process journey. Risks can be identified in a number of ways - from a person spotting a risk while doing their job to a team during a workshop.

At this stage the intention is to describe the risk with a focus on:

The **risk event** – *a summary explaining what may or may not occur*
The **cause(s)** – *those factors that will lead to the risk event occurring*
The **effect(s) / consequence(s)** – *the likely impact on activities and outcomes if the risk event does occur*

By methodically working through the risk event and identifying the cause(s) and effect(s) it encourages a better understanding of the risk and a more structured definition of the risk. It is not always easy to describe risks, however the key point is that everyone understands what is meant by the risk and the description is sufficient to ensure an effective understanding of the risk moving forwards.

Some examples of causes of risk are:

- Failure to……..
- Loss of……..
- Insufficient.....
- Non-compliance with….
- Reduction in……
- Conflict between……
- Inability to……
- Reliance on……
- Disruption to……..
- Inadequate……
- Increase in……
- Delay in……..

The effects or consequences of risks can be numerous, and some examples are:

- Service disruption
- Impaired performance
- Management distraction
- Breach of contract
- Fines and penalties
- Loss of assets
- Financial cost
- Damaged reputation
- Health and Safety failings

Risk Register Updated:
At the end of this step the risk register should be populated with the:

- *Risk Title (the risk event)*
- *Cause*
- *Effect*
- *An initial Risk Owner – the person best placed to manage the risk*
- *Unique ID (provided by the Risk Manager)*

5 Risk Assessment

Risk assessment categorises risks according to **likelihood** of occurrence and **impact** on the organisation using a scoring-based system.

The **likelihood** is an estimate of the probability that the risk will occur. It takes into account any existing controls currently in place to help mitigate the risk from occurring. For example, applying the latest software patches to IT equipment is a control measure to reduce the chances of having computer viruses.

Shown below the likelihood is the current best assessment of the risk on a scale of 1-5.

Fig 3 - Likelihood criteria for risks

Level	Likelihood	Odds
1	Rare	<10%
2	Unlikely	10% to 29%
3	Possible	30% to 69%
4	Likely	70% to 90%
5	Very Likely	>90%

NOTE : It is important to understand that the goal is not to have the most accurate scoring but ensure that there is a prioritisation of risks. This allows for the allocation of resources focused on managing the most significant risks.

The **impact** is the negative effect that the risk could have on the organisation. Any existing controls to help manage the impact of the risk should be taken into account when undertaking the scoring assessment. For example, a business continuity plan would not change the likelihood of a risk occurring but is designed to reduce the impact.

The scoring is on a scale of 1-5 and is the best assessment based on the known risk information. To aid scoring for the Risk Owner, an impact criteria matrix is used, as shown in Fig 4. The criteria are only a guide for the Risk Owner to get a better 'feel' for the risks relative impact and thereby providing a consistent level of evaluation and ranking of risk across the organisation. It is not intended to be an exhaustive list as there are a multitude of impact areas such as governance, environment etc.

Fig 4 - Impact criteria for risks

IMPACT					
Level	**Impact**	**Financial (revenue)**	**Residents**	**Reputational**	**Performance**
1	Minimal	<£100k	Minimal impact on a small proportion of the population	Has no negative impact on reputation and no media interest	Minimal impact on achievement of one or more SCC priority objectives
2	Minor	£100K to £1m	Minor impact on a small proportion of the population	Minor damages in a limited area. May have localised, low level negative impact on reputation and generates low level of complaints	Minor impact on achievement of one or more SCC priority objectives
3	Moderate	£1m-£2.5m	Moderate impact on a large (or particularly vulnerable group) proportion of the population	Moderate damages but widespead. Significant localised low level negative impact on the organisations reputation which generates limited complaints.	Moderate impact on achievement of one or more SCC priority objectives
4	Major	>£2.5m to £10m	Major impact on a large (or particularly vulnerable group) proportion of population	Major damage to the reputation of the organisation. Generates significant number of complaints and likely loss of public confidence. Unwanted local or possibly national media attention.	Major impact on achievement of one or more SCC priority objectives
5	Severe	>£10m	Serious long term impact on a large (or particularly vulnerable group) proportion of population	Serious damage to the reputation of the organisation. Large number of complaints. National media coverage. Possible government intervention.	Serious long term impact on achievement of one or more SCC priority objectives

Once the risk likelihood score and impact score have been determined, they combine to provide an overall risk score (by multiplying the impact by the likelihood). This allows for a relative ranking of risks and a better focus on prioritising the most significant risks (with resources allocated accordingly).

Risk Register Updated:

At the end of this step the risk register should be populated with the:

- *Existing management controls to reduce the likelihood or impact of the risk*
- *Likelihood score*
- *Impact score*
- *Overall Risk Score (likelihood x impact)*

6 Risk Treatment

Risk treatment involves looking at the options to help mitigate the risk and taking the most appropriate actions. Very often the first idea (or option) is the most expensive and it is important to consider alternatives. The intention is to consider the cost-benefits of each option and then select the most appropriate to either reduce the likelihood of occurrence or the impact.

There are essentially 4 main treatment option, shown below in Fig 4:

Fig 5 - Risk Management treatment options

Activity / Option		Mitigation
Terminate	Stop what is being done.	The specific actions to be taken to control the risk
Treat	Reduce the likelihood or impact of the risk occurring.	
Transfer	Pass to another service best placed to deal with mitigations but ownership of the risk still lies with the original service. *One example would be insurance.*	The reasons for the transfer and the name of the service provider that the risk is being transferred to.
Tolerate	Do nothing because the cost outweighs the benefits and/or an element of the risk is outside our control.	The specific reasons / rationale for tolerating the risk.

NOTE: When considering the options, more than one mitigation may be appropriate.

Risk Register Updated:

At the end of this step the risk register should be populated with the:

- *Planned Enhancements to Controls (Actions) – treatment option(s) to further mitigate the risk*
- *Target Date(s) - The date when the action(s) should be completed by*

7 Risk Monitoring and Reporting

Effective risk monitoring and reporting is essential for informed decision-making and ensuring that the right actions are taken to drive improvement.

Risks must be regularly monitored to track progress, review the effectiveness of existing controls and consider any other factors that may impact the (level of) risk. The frequency of risk reviews will depend on the type of risks being assessed and the area that the risk sits within. For many parts of the organisation, the review of the risk register will be a standing item on the agenda. Nevertheless, all risks in a risk register must be reviewed every quarterly (at the very least) by the Risk Owner.

In addition to risk monitoring by the Risk Owner, a number of other stakeholders are likely to need to be kept informed on the risk status and contribute as required. Below shows some of the monitoring that takes place in the Council based on the risk hierarchy to support good risk management and good governance.

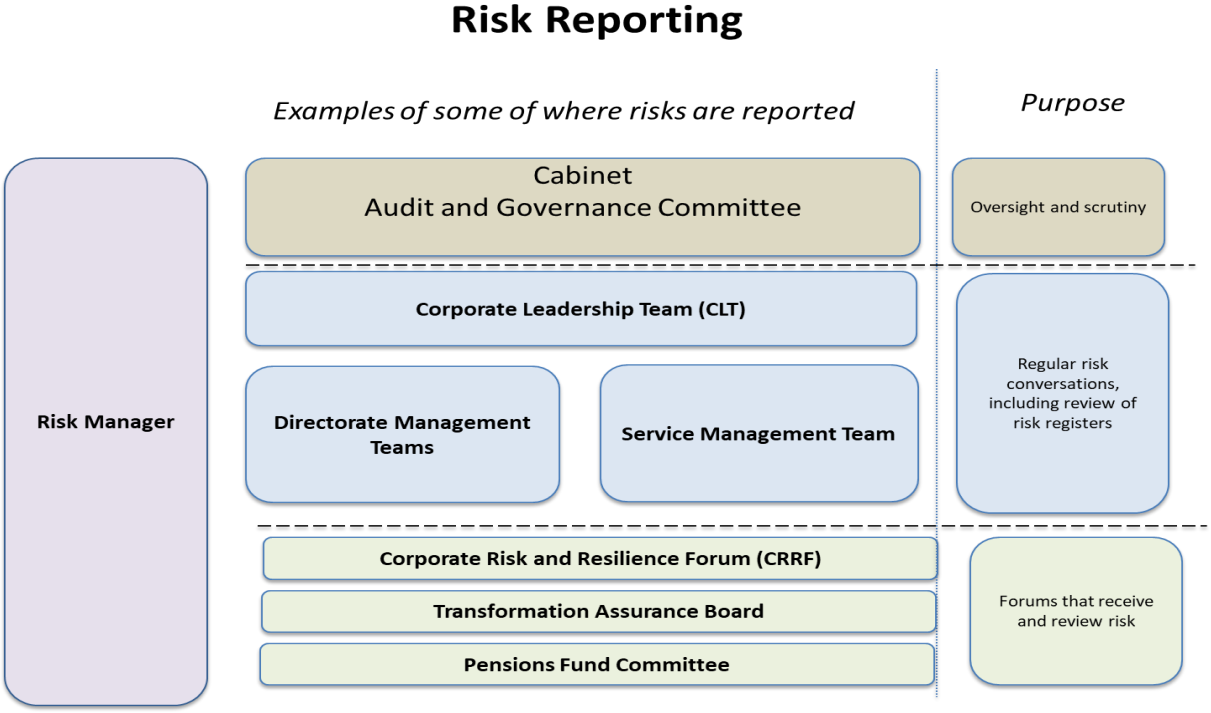
Risk Level / Hierarchy	Risk Monitoring
Strategic	• Corporate Risk Register reviewed by Corporate Leadership Team (monthly standing agenda item). New risks added if appropriate or removed or downgraded to departmental level. • AGC consider the Corporate Risk Register (standing agenda item) to provide oversight • Deep dives undertaken on risks to provide wider perspective and understanding
Directorate	• Risks reviewed and updated by Head of Directorate and their direct reports. • Risks escalated (via Head of Directorate or via Risk Manager), removed or downgraded
Service	• Risks reviewed and updated by Head of Service and their direct reports • Risks escalated (via Head of Service or via Risk Manager) or removed

Reports provide stakeholders a view on the current state of specific risks. Essentially there are 2 types of reporting:

- **Pre-defined reports** which are in the same format and provided to regular committees or other meetings. These will typically be undertaken by the overall responsible for that specific risk register.
- **Ad-hoc risk reports** on the status of risk. Typically, these will be spanning different parts of the organisation and are normally undertaken by the Risk Manager.

Below are some of the interested parts of Surrey County Council that require risk reports. While it is not a comprehensive list it does reflect that there are a large number of stakeholders that require risk information.

Fig 6 – Overview of some of the stakeholders that require risk information



It is **IMPORTANT** that anyone providing a risk report understands that there may be content which could be confidential. For example, the mitigations may cover commercially sensitive information or could be used to by-pass intended safeguards. Therefore, there must be a clear understanding of why the report is needed, what content requirement / risk information is needed, and who will have access to the report.

Typically a risk report as a minimum should show:

- The Title of the Risk
- The Owner of the Risk

Additional information may be made available such as:

- The cause(s) of the risk and the effect(s) on the organisation if it were to occur
- The current likelihood and impact if the risk
- The current control(s) in place to stop the risk from occurring
- The planned mitigation(s) to further reduce the likelihood or impact of the risk
- The due date(s) for completion of the mitigation

Risk Register Updated:

At the end if this step the risk register should be reviewed and any changes / updates made

Risk register Annex A

A risk register with a worked example

Risk ID	Risk Title	Causes	Effect	Risk Owner	Likelihood (1-5)	Impact (1-5)	Overall Score	Key Existing Management Controls	Planned Enhancements to Controls (Actions)	Target Date
Unique ref. no. to be provided by Risk Manager	*A short summary explain the risk*	*The reason(s) giving rise to the risk*	*What would happen if the risk occurred ?*	*Name of person owning/managing the risk*	*see risk matrix to help scoring*	*see risk matrix to help scoring*	*Calculation (Likelihood X Impact)*	*Controls that are already in place to stop the risk from occurring*	*Actions planned to further mitigate the risk*	*Month & Year*
Example :	There is a risk of a deliberate and / or targeted cyber attack compromising IT systems and critical IT infrastructure	- A deliberate attack by a cyber criminal or insider attack by a disgruntled employee or ex-employee. - State linked cyber crime attacks – a local government organisation can be viewed as less secure and a link into national government systems. - Lack of understanding amongst workforce of the potential cyber threats. - Failure of staff to adhere to the council's cyber security policies, procedures and guidance (behavioural and technical). - Legacy infrastructure and systems, that become increasingly vulnerable to exploitation as threats become more sophisticated and targeted.	- An immediate disruption to services if systems are unavailable. - Loss of access to individual resident's records, creating a risk of harm to their health and wellbeing. - Loss of access to operational data e.g. payroll data, payment data for suppliers, case files etc. - Financial cost of the immediate response e.g. rebuilding systems and restoring data. - Financial cost of longer term recovery e.g. potentially buying new infrastructure and strengthening resilience to cyber attacks. - Damage to reputation / loss of trust amongst the residents of Surrey, and partner organisations.	A.Smith	1	4	4	- Protective systems Firewalls, anti-virus, internet scanning in place - Inhouse security monitoring and penetration testing - Systems have latest patches applied - Cyber liability insurance in place - User access controls limits access to data - Business Continuity Plan in place to enable support of key services	- revised IT incident management policy being developed - internal audit planned and will undertake remedial work if identified	Oct. 2021 Jan. 2022

Area	Guidance
Risk ID	All risks must have a unique risk reference
Risk Title	A short summary explaining the risk
Cause	The reason(s) giving rise to the risk
Effect	What would happen if the risk occurred?
Risk Owner	The person best placed to own and manage the risk
Likelihood	The probability rating of the risk occurring
Impact	The rating of the risk effect to the organisation
Overall Score	Rating calculated by Likelihood x Impact
Key Existing Management Controls	Measures currently in place to reduce the likelihood or impact of the risk occurring
Planned Enhancements to Controls (Actions)	Further actions planned to help mitigate the risk to an acceptable level
Target Due	The deadline by which the mitigating actions should be completed