Risk Management Framework

February 2019

Introduction

Risk management is the process that we adopt to identify, evaluate and control risks. A risk is ***a potential future event that, if it materialises, has an effect on the achievement of our objectives***.

By having arrangements in place to identify and manage our risks, we increase the chances of achieving our objectives, and reduce the chance of failure. Effective risk management also increases our ability to cope with developing and uncertain events. The only thing constant is change; risk management helps us to anticipate, plan for and react to those changes.

This guide sets out the Council's risk management process. As you work through the guide it will take you through each stage of the process which can be illustrated as follows:

Templates and examples are available to assist you as you capture and assess your risks. The guide assumes no prior knowledge of risk management and can either be used in full, or in part based on experience. An FAQ and worked example section can be found in **LINK**

If you have any questions about this guidance, or would like additional support, then please contact a member of the Mid Kent Audit Team – contact details can be found in **Appendix III**.

Step 0 – Clarify your Objectives

A risk is an event that could affect the achievement of your objectives. So, before you can assess what stands in your way you need to know where you're going. What are your ***objectives***?

- **What** are you seeking to achieve?
- by **When**? And
- **Who** is responsible for achieving them?

This includes understanding what the Council wants to achieve and the resources it has available – in both capacity and capability – to deliver. The Council has set out its corporate objectives in the ***Strategic Plan***, and services objectives are determined as part of the ***Service Planning*** process.

Our aim is that risk management fits in with and supports your objectives, which in turn support the objectives of the Council. This link between Council objectives, through departmental or service objectives is called the golden thread. When everyone at the Council is pulling in the same direction we will have a much greater chance of being able to achieve our shared goals.

Clarifying your objectives will allow a greater understanding of what will stop you achieving those objectives and what opportunities you need to grasp to meet your goals. Setting our your objectives clearly will also reveal links to internal and external stakeholders on whom you rely as well as other external factors that will impact your objectives.

Step 1 – Identify your Risks

The purpose of any risk identification exercise is to find the uncertain event that could impact on your objective. As time passes, the things we need to do will inevitably change. As such this step has two principal elements:

- ***Initial risk identification***, for example when embarking on a new project, following a major service change or creating a new service plan, and
- ***Continuous risk identification***: that is to say changes to existing risks, including those which become irrelevant over time, or changes in circumstances leading to new risks.

Common techniques used across the Council to identify risks are **horizon scanning**, **brainstorming**, **workshops** and **facilitated discussions**. Asking the following questions can help identify risks:

- If in a year from now we haven't achieved this objective, why – what could have stopped us?
- What could realistically go wrong?
- What do we need in order to achieve this objective? Do we depend on others to succeed?
- What opportunities might arise?

One of the most common pitfalls in identifying risks is to simply say the opposite of the objective – look instead for potential events or circumstances which could occur in the future. The below table illustrates what may or may not be considered to be a risk:

Objective	Potential Risk Statement	Is this a risk?
To provide the best services resources allow	Failing to provide the best services resources allow	✘ This is simply stating the opposite of the objective.
	Public are dissatisfied with Council services	✘ This is a statement of the potential ***impact*** of failing to meet the objective; not in itself a risk.
	A lack of suitably trained and available staff limiting ability to deliver efficient services	✓ This is a risk we can ***control*** by, for instance, making plans to keep training up to date and reviewing our staffing needs.
	The Government has reduced our funding	✘ This has already happened and so is an ***event*** to be managed. Risks look ahead to potential events and so involve at least some uncertainty.
	The Government sharply reduces future funding	✓ This is a risk over which we have little or no control, but we can assess ***likelihood*** and, if required, make ***contingency plans***.

When articulating your risk it is useful to capture the cause and consequence of the risk, i.e. as a result of [***cause***], [***risk***] could occur meaning [***consequence***]. So, for the above example one risk could read: *Government policy changes could result in a significant reduction in future funding, leading to a reduction in the quality of our service*.

Risk Types

As outlined in step 1, risks can be identified at various different points in time. The different types of risk that may be identified within the Council are:

- Corporate – risks that have a Council-wide effect or that effect the achievement of the Council's strategic priorities. These are usually identified annually in line with changes to the strategic plan.
- Operational – risks that effect the achievement of a services objectives, as identified through the service planning process.
- Project – risks relating to the delivery of a specific project, identified as part of the Council's project management approach.
- Procurement & Contract – risks associated with procurement activities or entering into a contractual arrangement. These are identified as part of procurement activities.
- Health & Safety – the risk that a person is harmed or suffers adverse health effects from exposure to a hazard. These are identified through the Council's Health & Safety approach.
- Business Continuity – the risk of a serious incident that impacts the Council. These are identified as part of the Council's Business Continuity Planning approach.

Risk Ownership

Once identified, it is essential that someone ***owns the risk***, taking principal responsibility for monitoring its course and tracking actions in response. Risk ownership is not the same as actually undertaking or being responsible for carrying out actions in response. Rather the role is aimed at ensuring necessary actions take place, otherwise there is a chance management actions may not be completed.

The best risk owner will usually be someone closely involved in delivering the area of the business where the risk arises.

The risks generated at this point should be captured in the ***risk register***. A template is available here **LINK.**

Step 2 – Evaluate your Risks

Having identified the risk, the next step is to understand how big it is. Risk evaluation incorporates two principal elements:

- **Impact** – That is to say how severely the organisation would be effected if the risk transpires. In other words if the forecast event actually happens then what will that do to the Council?
- **Likelihood** – This is a consideration of how likely it is that the risk will occur. In other words the probability that it will materialise and become an event that needs to be managed.

A key element of evaluating risks is establishing what controls are currently in place to manage the risk. This helps us to determine the 'business as usual' position, referred to as the ***current risk***.

A control is defined as *any action taken by management or other parties to manage risk and increase the likelihood that objectives and goals will be achieved*. There are different types of internal controls as described in the following table:

Control Category	Description	Examples
Preventative	Designed to limit the possibility of an undesirable outcome. These primarily manage the *likelihood* of the risk.	Financial Standing Orders Prior authorisation of expenditure Access controls (system / physical) Data retention and destruction
Directive	Designed to set desired outcomes and expectations. Can manage the risk *impact* or *likelihood*.	Policies and procedures Training and awareness Job descriptions Manuals
Detective	Designed to identify problems when undesirable events have occurred. These primarily manage the risk *impact*.	Analytical review Exception reporting Sample checking Physical checks
Corrective	Designed to correct and undesirable outcome, and prevent re-occurrence. These primarily manage the risk *impact*.	Restoration of backup files Insurance / compensation

Score Risks

Once the controls have been identified the risk can be evaluated – that is to say given a risk score. The overall score is obtained from multiplying the impact and likelihood scores.

Risk impact is considered across a number of different criteria, financial and non-financial. **The highest potential impact score should be taken as your overall impact score.** The criteria used to assess impact and likelihood can be found in **Appendix I** and should be used to guide your evaluation of each risk identified.

A worked example is provided in the FAQ at **LINK**. Document your existing controls and impact and likelihood scores in your ***risk register***.

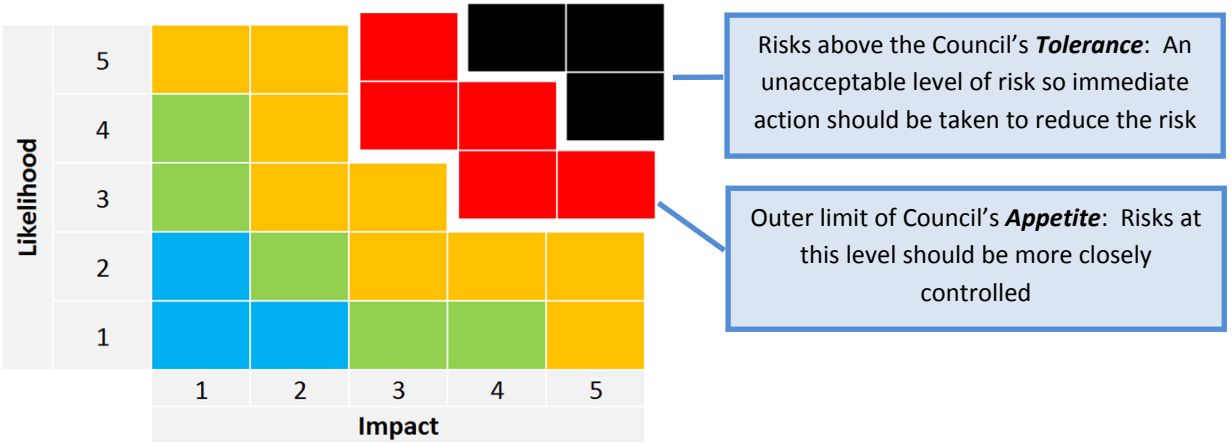
Step 3 – Respond to your Risks

Now you've identified your risks and established how big they are, you will need to decide what action (if any) you are going to take.

Risk Appetite Statement

Our ***risk appetite*** guides how much risk we are willing to seek or accept to achieve our objectives. We recognise effective risk management considers not just threats but also opportunities. So, our approach to risk is to seek the right opportunities and, where possible, minimise threats. Beyond our risk appetite is our ***risk tolerance***. This sets the level of risk that is unacceptable, whatever opportunities might follow. In such instances we will aim to reduce the risk to a level that is within our appetite.

We illustrate our risk appetite and tolerance in the matrix below. The **RED** area represents the outer limit of our risk appetite, and the **BLACK** area indicates the tolerance. As a Council we are not willing to take risks that have significant negative consequences on the achievement of our objectives.



Risk Response

There are four principal ways in which we can respond to risks, these are known collectively as 'the four Ts':

TREAT	TOLERATE	TRANSFER	TERMINATE
Put in place (or strengthen) controls - this is the most common way of manging risks.	Accepting the likelihood and consequences of the risk.	Shifting the risk, in whole or in part, to a third party.	Deciding to cease the activity which causes the risk.

The following table outlines what risk owners should do to respond to their identified risks:

Risk Rating		Guidance to Risk Owners
20-25	Risks at this level sit above the tolerance of the Council and are of such magnitude that they form the Council's biggest risks. The Council is not willing to take risks at this level and action should be taken immediately to treat, transfer or terminate the risk.	Identify the actions and controls necessary to manage the risk down to an acceptable level. Report the risk to the Audit Team and your Director. If necessary, steps will be taken to collectively review the risk and identify any other possible mitigation (such as additional controls).
12-16	These risks are within the upper limit of risk appetite. While these risks can be tolerated, controls should be identified to bring the risk down to a more manageable level where possible. Alternatively consideration can be given to transferring or terminating the risk.	Identify controls to treat the risk impact / likelihood and seek to bring the risk down to a more acceptable level. If unsure about ways to manage the risk, consult with the Internal Audit team.
5-10	These risks sit on the borders of the Council's risk appetite and so while they don't pose an immediate threat, they are still risks that should remain under review. If the impact or likelihood increases then risk owners should seek to manage the increase.	Keep these risks on the radar and update as and when changes are made, or if controls are implemented. Movement in risks should be monitored, for instance featuring as part of a standing management meeting agenda.
3-4	These are low level risks that could impede or hinder achievement of objectives. Due to the relative low level it is unlikely that additional controls will be identified to respond to the risk.	Keep these risks on your register and formally review at least once a year to make sure that the impact and likelihood continues to pose a low level.
1-2	Minor level risks with little consequence but not to be overlooked completely. They are enough of a risk to have been assessed through the process, but unlikely to prevent the achievement of objectives.	No actions required but keep the risk on your risk register and review annually as part of the service planning process.

Depending on how you have decided to respond to your risk the following action will need to be taken:

- Where you have decided to **TREAT** your risk: document your planned controls / actions in your risk register and re-score impact and/or likelihood. This will give you your ***mitigated*** risk rating.
- If you have decided to **TOLERATE** the risk no further action is necessary. The risk register will capture the risk and its' existing controls and the ***current*** and ***mitigated*** scores will be the same.
- For **TERMINATED** risks, the risk should remain in the risk register until the activity causing the risk has been stopped. You may want to capture what action is being taken to terminate the activity. Once terminated the risk should be removed from the risk register.
- Where you decide to **TRASFER** (in whole or in part) the risk you will need to consider what risk remains to the Council. Capture the transfer as a planned action in the risk register and re-score impact and/or likelihood. This will give you your ***mitigated*** risk rating. Once the risk has been transferred you may want to consider whether any risks relating to the transfer need to be recorded in the risk register.

Document your decided course of action and (where necessary) impact and likelihood scores in your ***risk register***.

Step 4 – Monitor and Report on your Risks

Once you have identified your risks, determined the current and (if required) mitigated risk scores, and recorded this information on the ***risk register***, send the completed registers to ***internal audit*** using the contact details in **Appendix III**.

Internal Audit will maintain a register of all the Council's risks which will be used to report on key risks over the course of the year. The risk register will be updated periodically so please continue to send risk updates to internal audit as they arise.

The frequency with which we monitor risks is set out in the following matrix:

		Impact				
		1 *Minimal*	**2 *Minor***	**3 *Moderate***	**4 *Major***	**5 *Catastrophic***
Likelihood	**5 *Almost Certain***	*Monitor Quarterly*	*Monitor Quarterly*	*Monitor Monthly*	*CLT Monitor Monthly*	*CLT Monitor Monthly*
	4 *Likely*	*Monitor 6-Monthly / Annually*	*Monitor Quarterly*	*Monitor Monthly*	*Monitor Monthly*	*CLT Monitor Monthly*
	3 *Possible*	*Monitor 6-Monthly / Annually*	*Monitor Quarterly*	*Monitor Quarterly*	*Monitor Monthly*	*Monitor Monthly*
	2 *Unlikely*	*No Action Required*	*Monitor 6-Monthly / Annually*	*Monitor Quarterly*	*Monitor Quarterly*	*Monitor Quarterly*
	1 *Rare*	*No Action Required*	*No Action Required*	*Monitor 6-Monthly / Annually*	*Monitor 6-Monthly / Annually*	*Monitor Quarterly*

monitoring and reporting activities in place to ensure that our risks are kept under control are:

- Corporate Leadership Team actively monitor all **Black** risks, e.g. through separate monthly reports on the risk area.
- Quarterly reporting to Corporate Leadership Team on all corporate and high-level (**Red** / **Black**) operational risks.
- 6-monthly reporting to Wider Leadership Team on all corporate risks and the overall risk profile.
- 6-monthly reporting to Policy & Resources Committee on all corporate risks and the overall risk profile.
- Annual reports to Audit, Governance & Standards Committee on the effectiveness of the risk management process.
- Risk registers are sent to quarterly to directors and heads of service to enable broader consideration of risk across the Council.
- Mid Kent Audit facilitate the review and update of risk actions (as per your risk register) during the year for and high-level (**Red** / **Black**) risks.

If a critical or significant risk arises, it is important that Officers and Members are fully informed about the risk and how the Council is responding to and managing that risk. A number of mechanisms are in place to allow for this communication to happen if risks fall outside of the usual reporting process. For example, formal or informal communication with Committee Chairs and Group Leaders; issuing a briefing; adding an urgent item to an already scheduled meeting; or submitting a formal item to the Urgency Committee. Similarly, Members can raise key risk issues through their regular interaction with officers either directly or via their Group.

We all have a duty to be aware of, and manage the risks that may prevent us from delivering services. The formal consideration of risk is undertaken as part of the service and strategic planning processes, and so we expect the Framework to be used predominantly by managers, heads of service and the corporate leadership team. **Appendix II** outlines the respective roles and responsibilities of those involved in the risk management process.