

BRECKLAND COUNCIL Risk Management Process Guide

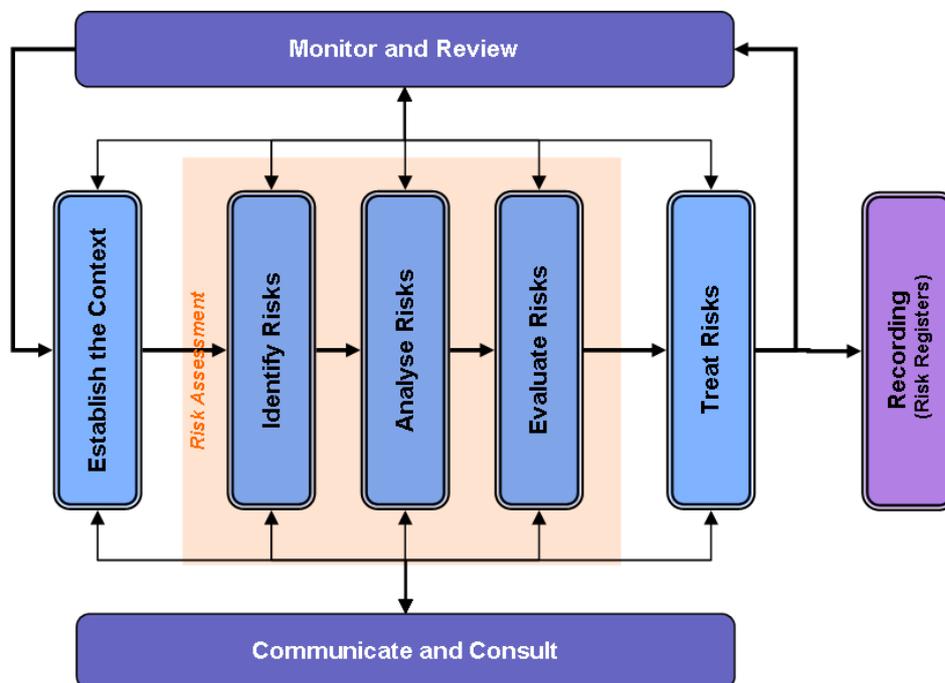
Introduction

Every aspect of the Council’s work involves some risk: policy making, decision taking, action and implementation, regulation and spending. There is an increasing expectation that we need to manage these risks well, to cut waste and inefficiency, and reduce unanticipated problems that undermine trust. Successful organisations are not afraid to take risks; unsuccessful organisations take risks without understanding them. Making the most of opportunities to improve public services, involves some amount of risk taking.

This process guide is a step by step guide for the process of identifying, assessing, addressing, reviewing and reporting risks. It should be read in accordance with the council’s risk management policy. It is owned by the Performance team and will be regularly reviewed and updated in line with any amendments to the risk management policy.

The Risk Management Process – Steps in the process

Our risk management processes will be an integral part of management of the organisation, with the objective of embedding the risk management process into our culture and practices. We will take elements of best practice and tailor them to the business processes and needs of the organisation. The risk management process provides a standardised and consistent approach to the management of risk across the organisation.



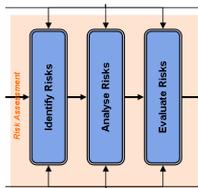
Step 1 - Establishing the risk context



Establishing the risk context consists of establishing the basic parameters for managing risk and sets the scope and criteria for the rest of the risk management process. This first step is an essential step prior to risk identification. It involves considering:

- What we are looking at – corporate or service objectives, project or partnership objectives, budgets or policies, procurement or commissioning, options for decisions. It is also important to consider the critical activities identified through the business continuity process.
- Who will be involved – internal and/or external stakeholders
- Who will be responsible for the process, we will need to define responsibilities for review, monitoring and reporting.
- The risk criteria and appetite – risk types, likelihood and impact matrices, and risk treatment can all be found in this document. These risk management tools will assist through all the steps of the risk process.

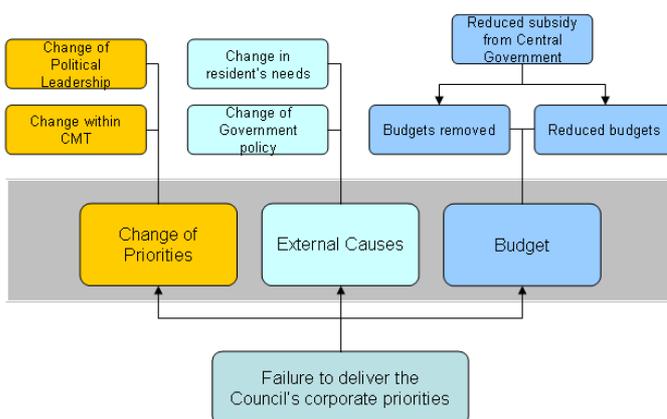
Step 2 - Identification, analysis and evaluation of risks.



The second stage of the risk process consists of identifying, analysing and evaluating the risks of the council and assessing whether these risks are under control.

A) Risk Identification

This is about describing the risk(s) in order to fully understand the potential chance of something happening that might affect the achievement of our objectives and what impact it will have. It is defined as the combination of the probability (likelihood) of an event and its consequences (impact).



It may be useful to consider the source of risk, for example, political risks, financial risks, etc. A list of example risk sources can be found below.

Once identified, all risks are entered into the relevant Strategic, Operational or Programme / Project / Partnership risk registers.

Figure 3 - Example of identification of the causes of a risk.

Risks can bring about both positive and negative impacts. It is equally as important to identify risks associated with not pursuing an **opportunity**, as it is to identify risks that present a **threat** to the council.

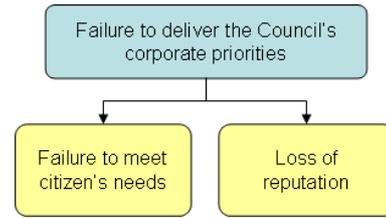


Figure 4 - Example of identification of the consequences of a risk

It is important that the risk is clearly described, this will include what the event or situation may be, how it could affect the council, when it could affect the council, why it could affect the council and to what extent. The fuller the description the easier it will be to estimate impact and likelihood scores. It is also important that the people who carry out this step have the correct level of knowledge and understanding of any potential risks.

Methods that can be used to complete this step include workshops, one to one meetings, the use of historical information and lessons learnt.

Risk Sources

Strategic	Operational
Risk & Description	Risk & Description
Political	“Job”
Risks associated with the organisation’s ability to deliver either central government policy or meet the administration’s manifesto commitments.	Risks specific to the activity of the departments within the organisation.
Financial	Financial
Risks associated with the organisations inability to respond to financial commitments. These may be: External - e.g. interest rates, exchange rates, inflation. Internal – e.g. budgetary pressures, adequacy of insurance cover, consequences of proposed investment decisions.	Risks associated with the effective management and control of the finances of the organisation and instances of fraud, particularly in key financial/operational areas such as procurement, insurance, benefits and partnerships and in the management of personal data and the prevention of identity fraud.
Social	Reputation
Risks associated with demographic or socio-demographic changes affecting the organisation’s ability to carry out its tasks (e.g. ability to recruit, retain and motivate staff with the required skills in the required number).	Risks associated with the reputation of the organisation and the public’s perception of its efficiency or legitimacy.
Technological	Technological
Risks associated with the organisation’s inability to adapt to progress or to use the latest technologies, to meet a new demand resulting from major technological change.	Risks associated with the malfunction or obsolescence of technological equipment (IT systems, equipment, etc).

Legislative	Legislative
Risks associated with major changes within the legislation or regulations applied to the organisation's field of activity (e.g. Human Rights Act, Freedom of Information Act, etc).	Risks associated with the potential non-compliance with legislation.
Environmental	Environmental
Risks associated with the environmental consequences of progressing the organisation's strategic objectives (e.g. recycling, landfill requirements, emissions, etc) or the impacts of ongoing operations (e.g. pollution, noise, energy efficiency).	Risks associated with the pollution and noise generated, or the energy efficiency of the operations carried out by the organisation.
Competitiveness	Contractual
Risks associated with the competitiveness of the services delivered by the organisation, in terms of cost and quality.	Risks associated with the inability of the co-contracting parties to deliver products/services in the technical and financial conditions expected.
Customer / Citizens / Clients	
Risks associated with the organisation's inability to meet expectations and the new needs of customers / citizens / clients.	

Assign a Risk Owner

All risks, once identified, should be assigned to an owner who has responsibility for ensuring that the risk is managed and monitored over time. A risk owner, in line with their accountability for managing the risk, should have sufficient authority to ensure that the risk is effectively managed; the risk owner may not be the person who actually takes the action to address the risk.

Risk owners are responsible for:

- Ensuring that appropriate resources and importance are allocated to the process;
- Confirming the existence and effectiveness of the current mitigating actions and ensuring that any proposed mitigating actions are implemented;
- Providing assurance that the risks for which they are the Risk Owner are being effectively managed.

B) Risk Analysis

Risk analysis is concerned with developing an understanding of each risk we have identified, assessing the chances of it happening (**likelihood**) and the consequences if it does (**impact**).

I. Assessing Likelihood and Impact

Once the risks have been identified the likelihood of risk occurring and the impact they will have if they occur must be assessed. It is important to note that the likelihood and impact of the risks identified need to be considered and ranked on the worse case credible scenario with existing controls in place.

Calculating the Inherent Risk Score

There will probably already be measures in place to minimise any identified risks – known as mitigating actions. However, it is important to bear in mind that in the first instance, risks are assessed on the basis that there are no measures in place or on the basis that any existing measures are not operating effectively. In other words we are seeking to ascertain the worst case scenario if the risk were to occur. This is known as the “inherent” risk.

The Risk Matrix below describes the agreed criteria you must use to assess whether likelihood and impact are high, medium or low.

Calculating the Current Risk Score

The likelihood and impact of the identified risks should also be assessed following the identification of control measures / mitigation plans in step III. This assessment will ascertain the “current” risk score, i.e. the remaining level of risk after control measures / mitigation action has been taken. The

II. Risk Proximity

When considering risk likelihood, another aspect to consider is when the risk might occur. Some risk will be predicted to be further away than others and so attention should be focused on the more immediate risks first. This prediction is called the risk’s proximity.

III. Control Measures / Mitigation Plans

When evaluating risk, there is a need to identify existing control measures that are currently in place to manage the risks and any new mitigation plans (countermeasures) that need to be put in place to manage the risk.

IV. Risk Matrix

When evaluating the likelihood and impact of risks through meetings, workshops or updating the performance management system, the risk matrix can be used to help plot risks. The risk matrix can be seen below.

V. Risk Tolerance

When identifying risk tolerance, a risk tolerance line can be plotted on the risk matrix to show that any risks above this line needs to be referred upwards for decisions.

The Council has decided that any Strategic or Operational risks that are scored at level 6 to 9 will be viewed as unacceptable in the first instance and must be “treated” with Senior Management involvement. At this stage some form of *cost / benefit analysis* may be needed to ensure that the cost of further risk mitigation action does not outweigh the cost of tolerating or accepting the risk.

C) Risk Evaluation

Risk evaluation involves making a decision about the level or priority of each risk. Risks are prioritised for attention by placing them into the following levels relating to their final risk scores:

The Council uses a RAG (red, amber, green) status to evaluate these factors. Each colour has a different meaning and can be summarised as follows:

RAG Status	Level of risk	Description
High Risk	6 - 9	Immediate action required, Senior Management must be involved and management responsibility specified
Medium Risk	3 - 4	Management responsibility specified and managed by specific monitoring or response procedures
Low Risk	1 - 2	Manage by routine procedures, unlikely to need specific or significant application of resources

Impact	High 3	3	6	9
	Medium 2	2	4	6
	Low 1	1	2	3
		Low 1	Medium 2	High 3
		Likelihood		

Measures of Likelihood and Impact

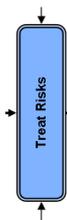
Likelihood

Score	Description	Definition
3	Red (High)	Has happened in the past year ; or Is expected to happen in the next year More than 50% probability
2	Amber (Medium)	Has happened in the past 2 – 5 years ; or Is expected to happen in the next 2-5 years Between 25% to 50% probability
1	Green (Low)	Has not happened in the past 5 years or more ; or Is not expected to happen in the next 5 years or more Between 1% to 25% probability

Impact

Score	Description	Example Detail
3	Red (High)	Death or life threatening Serious service failure impacts on vulnerable groups Negative <u>national</u> publicity, highly damaging, severe loss of public confidence Serious impact felt across more than one Directorate Legal action almost certain and difficult to defend Financial impact in excess of £100,000 Non-compliance with law resulting in imprisonment Loss of, or permanent damage to, 'priority' environmental/historic resources
2	Amber (Medium)	Extensive, permanent/long term injury or long term sick Service failure impacts on property or non-vulnerable groups Negative <u>local</u> publicity, some loss of confidence, needs careful public relations Expected impact, but manageable within Directorate contingency plans Legal action expected Financial impact between £50,000 - £100,000 Non-compliance with law resulting in fines Recoverable damage to 'priority', or loss of 'non-priority', environmental/historic resources
1	Green (Low)	Short term sick absence, first aid or medical treatment required Some risk to normal service but manageable within contingency arrangements Little if any scope for impact on vulnerable groups Possible negative customer complaints, unlikely to cause adverse publicity, no damage to reputation Possible impact, but manageable locally by Service Managers Legal action possible but unlikely and defensible Financial impact less than £50,000 Non-compliance with regulations / standards or local procedures resulting in disciplinary action. Recoverable damage to 'non-priority' environmental/historic resources

Step 3 – Treatment of risks



Once a risk has been evaluated and adequate control measures identified and assessed, decisions need to be made on how to treat the risk in order to improve the outcome. This involves either improving existing controls or developing and implementing new controls.

There are a number of treatment options available:

Treatment	Description
Avoid a threat (Or, exploit an opportunity)	This option is about making the uncertain situation certain by removing the risk. This can often be achieved by removing the cause of a threat, or by implementing the cause of an opportunity.
Reduce a threat (Or, enhance an opportunity)	This option chooses definite action now to change the probability and/or the impact of the risk. The term mitigate is relevant when discussing reduction of a threat, i.e. making the threat less likely to occur and /or reducing the impact if it did. Enhancing an opportunity is the reverse process i.e. making the opportunity more likely to occur and/or increasing the impact if it did.
Transfer the risk	Transfer is an option that aims to pass part of the risk to a third party. Insurance is the classic form of transfer, where the insurer picks up the risk cost, but the insured retains the impact on other objectives e.g. time delay.
Share the risk	Share is an option that is different in nature from the transfer response. It seeks multiple parties to share the risk on a pain/gain share basis.
Accept the risk	The accept option means that the organisation will “take the chance” that the risk will occur, with its full impact if it did. There is no change to residual risk.
Prepare contingent plans	This option involves preparing plans now, but not taking action now. This is most usually associated with the accept option, preparing contingent plans in this instance is saying “we will accept the risk for now, but we’ll make a plan for what we’ll do if the situation changes”. This is essentially a fallback plan.

Recording Risks

All risk management activity should be recorded. The performance management system will be the key tool for the capture, analysis and ongoing review of all risks.

All initial risk analysis will need to be captured on manual forms, the risk register template in this document has been designed to assist with this process. Once captured in this format, any new or amended risks will be added to the performance management system.

Step 4 – Monitor and Review



The initial aim for this step is to ensure that the planned responses to the identified risk have been implemented, understanding if they have been successful, identifying and assessing any residual risks where responses have not been entirely successful and planning and implementing additional risk countermeasures.

The review process will take place at various levels. All risk will be reviewed to ensure that they are still valid, that risk treatments are working and that target dates for dealing with risk are still valid. There is no specific frequency with which all risks will be monitored; this will be dependent upon the nature and type of the risk. The table below sets out the way in which different types of risk will be monitored and reviewed:

What	Why	Who	When
Strategic Risk Registers	To monitor progress of risk treatments and to add or remove risks from the register	Corporate Management Team	Quarterly
Operational Risk Registers (Dept. & Service risk registers)	To monitor progress of risk treatments and to add or remove risks from the register. To escalate existing risks if necessary.	Service Management	Monthly
Programme / Project Risk Registers	To monitor progress of risk treatments and to add or remove risks from the register. To escalate existing risks if necessary.	Programme & Project Managers	As agreed by the relevant Programme / Project boards
Partnership / Contract Risk Registers	To monitor progress of risk treatments and to add or remove risks from the register. To escalate existing risks if necessary.	Partnership / Contract Managers	As agreed by the Partnership boards.

Risk Management Tools and Techniques

A number of risk management tools and techniques can be found on the intranet to assist in undertaking risk assessment and analysis. These tools and techniques are based on current best practice techniques and will be kept up to date by the performance team. If you require any assistance with these tools and techniques or any other element of this process guide, please contact a member of the performance team - performance@breckland.gov.uk.

Risk Register Template

Risk Ref	Council Priority	Risk Owner	Risk Description	Risk Consequences	Inherent			Control Measures (what is being done to avoid this)	Proximity (when is the risk likely to occur)	Cost / Benefit (Are further controls cost effective?)	Current			Mitigation Plan (what will be done if this occurs)
					Impact	Likelihood	Rating				Impact	Likelihood	Rating	

Glossary of Terms

Term	Definition
Consequence	Outcome of an event affecting objectives.
Control	Measure that is modifying the risk.
Establishing the Context	Defining the external and internal parameters to be taken into account when managing risk.
External Context	External environment in which the organisation seeks to achieve its objectives.
Internal Context	Internal environment in which the organisation seeks to achieve its objectives.
Impact	Cost or consequences to the Council if the risk happens.
Likelihood	Chance of something happening.
Mitigation	Plans intended for use, only if required e.g. if a risk response or control measure is not successful.
Monitoring	Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected.
Proximity	When considering risk likelihood, another aspect to consider is when the risk might occur. Some risk will be predicted to be further away than others and so attention should be focused on the more immediate risks first. This prediction is called the risk's proximity.
Residual Risk	Remaining risk after all control measures are in place.
Review	Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.
Risk	Effect of uncertainty on objectives.
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation.
Risk Management	Co-ordinated activities to direct and control an organisation with regard to risk.
Risk Owner	Person or entity with the accountability and authority to manage a risk.
Risk Treatment	<p>Process to modify risk. This can involve:</p> <ul style="list-style-type: none"> • Avoiding the risk by deciding not to start or continue the activity giving rise to the risk • Taking or increasing risk in order to pursue an opportunity • Removing the risk source • Changing the likelihood • Changing the consequences • Sharing the risk with another party or parties (inc. contracts and risk financing) • Retaining the risk by informed decision.