IPSWICH BOROUGH COUNCIL

APPENDIX 3

RISK MANAGEMENT TOOLKIT

V5 February 2024

Contents

1. Risk management toolkit

The Risk management process outlined within this toolkit should be used as a guide to best practice in managing risks which could impact strategic priorities, operational activities (e.g., delivery of actions identified in directorate or service plans) and delivery of programmes and projects.

Risk management activity will happen at different levels within the organisation and for different purposes. You are identifying the risks that may affect the delivery of these objectives. A risk is where there is uncertainty of the outcome which may have a positive or negative effect on the achievement of the desired outcome, e.g., the objective.

A step-by-step guide follows to enable you to understand the risk management process.

2. Establishing the context and Identifying objectives

The starting point for risk management is to ensure that there is a clear understanding and agreement on the objectives being considered (i.e., overarching corporate objectives, service, or project objectives, etc.). In this regard, risks are managed via a series of risk registers across the following levels within the organisation:

Corporate Level: the key risks facing the authority and the achievement of its corporate objectives.

The Corporate Risk Register (CRR) is reviewed by the Corporate Management Team (CMT) on a quarterly basis any new risks are incorporated into a revised version of the CRR. Risk owners for Corporate Risks are generally held at Director or Assistant Director level.

Service Level: the risks arising from service operations.

Service Area risks are considered as part of the service planning process and reviewed periodically by Assistant Directors and Heads of Service. High (red) risks are considered for potential inclusion in the Councils Corporate Risk Register on a quarterly basis.

Programme / Project Level: the risks from initial business case stage throughout the project lifecycle.

It is the responsibility of Project Managers to identify and ensure mitigation of risks relating to their project. These are reported via highlight reports for each project to the Programme Manager and to the relevant service to which the project relates. High (red) risks are considered for potential inclusion in the Councils Corporate Risk Register on a quarterly basis and should be escalated to Business Improvement team in the first instance.

The purpose of risk management is to manage the barriers which prevent an organisation from achieving its objectives.

The Council has developed a clear process for setting objectives through its corporate strategy, linking to business and service planning.

Within business and service plans it is important that objectives are SMART (specific, measurable, achievable, relevant, timed) and equally important to recognise how success against these objectives will be identified.

The same principles should be applied to council projects in that it will be impossible to manage based on aspirational targets and objectives.

Consideration should also be given to:

- partnership arrangements where complex risks might be involved through joint service provision where there are potential delays or quality issues.
- environment and climate change goals where risks and decisions might hinder the improvements to the environmental impact.
- Sustainability for the business .i.e., business continuity, financial sustainability

Examples -

To deliver the corporate strategy goals and aims
To provide services which are easy to access by all
To provide easily accessible information on all council services
To deliver planned efficiency savings
To travel by train from A to B for a meeting at a certain time

3. Identifying Risks

Once objectives have been specified, you will need to identify what will prevent those objectives from being achieved.

Risk management will take the form of an initial risk identification and should cover the following:

- Risks identified relate to objectives
- Include the case of the risk and its impact on the objective
- Try to identify all risks, those not included cannot be actively managed or monitored
- Consult stakeholders as their views may differ widely as to what constitutes risk
- Consider using a working group to identify risks
- Establish risk ‘ownership’, to reinforce ownership this should be a specific individual and not a group or committee

Once identified, the risks need to be described in sufficient detail and recorded in a consistent format to support effective decision making on the way that the risk is managed. It is crucial for risks to be defined properly at this stage. Failure to do so can result in confusion about the exact nature of the risk, ineffective risk controls being implemented, or the risk analysis being over or underestimated.

The description of the risk should include the following elements:

- Risk Title – a short and concise header for the risk

- Description – expanding on the risk title outlining the situation or event that exposes us to a risk.
- Risk Cause – also known as the trigger event. Situations or factors which result in the risk becoming a reality.
- Risk Effect - the likely consequences if the risk materialises (The negative impact - consider worst likely scenario)

When describing a risk try not to describe the impact of the risk as the risk itself or define risks with statements which are the converse of objectives. Focus upon the uncertain event that would result in those impacts.

Example - Objective: to travel by train from A to B for a meeting at a certain time

Failure to get from A to B in time for the meeting	X this is simply the converse of the objective
Being late and missing the meeting	X this is a statement of the impact of the risk, not the risk itself
There is no buffet on the train, so I get hungry	X this does not impact on achievement of the objective
Missing the train causes me to be late and miss the meeting	✓ this is a risk which can be controlled by making sure I allow plenty of time to get to the station
Severe weather prevents the train from running and me from getting to the meeting	✓ this is a risk which I cannot control, but against which I can make a contingency plan

The following tables give a summary of the most common categories used in risk identification. It provides a useful checklist against the range of potential risks which can arise both internally and externally and involving partner organisations.

4. External Factors

Arising from the external environment, not wholly within the organisation's control, but where action can be taken to mitigate the risk.

		Example -
Political	Change of government, cross-cutting policy decisions, machinery of government changes	May elections result in change of leadership at IBC
Economic	Ability to attract and retain staff in the labour market; exchange rates affect costs of international transactions; effect of global economy on the UK	Housing market downturn Interest rate rises

Social	Demographic change affects demand for services: stakeholder expectations change	Ageing population
Technological	Obsolescence of current systems; cost of procuring best technology available, opportunity arising from technological development	Cost of implementing new systems
Legal / Regulatory	EU requirements / laws which impose requirements	Health and Safety Employment legislation
Environmental	Buildings need to comply with changing standards Environmental Benefits	Disposal of rubbish and surplus equipment Green Travel Plan Climate Change Strategy and Carbon neutral goals

5. Operational

These relate to existing operations - both current delivery and building and maintaining capacity and capability.

		Example -
Service failure	Fail to deliver the service to the user within agreed / set times	Litter bins unemptied Housing repairs not carried out
Project delivery	Fail to deliver on time / budget / specification	Strategic Projects
Resources	Financial HR Information including the quality of data Physical assets	Insufficient funding, poor budget management Staff capacity, skills, recruitment, and retention Adequate for decision-making; protection of privacy Loss / damage / theft
Relationships	Delivery partners Customers / Service users Accountability	Non-commitment to relationship / clarity of roles Satisfaction with delivery To government, council tax payers
Operations	Overall capacity and capability to deliver	Recruitment, training, and development

Reputation	Confidence and trust which stakeholders have in the organisation	Adverse publicity
Governance	Regularity and propriety Compliance with relevant requirements Ethical considerations	Audit / Inspection regimes Keeping up to date with legislation, PI definitions Carbon reduction, travel plan, waste recycling
Scanning	Failure to identify threats and opportunities	Managing extremism
Resilience	Capacity of systems/accommodation/IT to withstand adverse impacts/crises Disaster recovery/contingency planning	Including war/terrorist attack Extreme weather
Security	Physical assets Information	Managing cyber security

6. Change

Risks created by decisions to pursue new endeavours beyond current capability.

		Example -
Capability	New targets challenge the organisation's capacity to deliver Ability to equip the organisation to deliver	Government legislation New council objectives
Corporate initiatives / Strategic Projects	Programmes for organisational or cultural change threaten capacity to deliver as well as providing opportunity to enhance capacity Programmes or projects that have not considered strategic commitments, leading to inability to deliver core strategies i.e., Climate Change strategy	Partnership working Environmental benefits & impacts Carbon Neutral

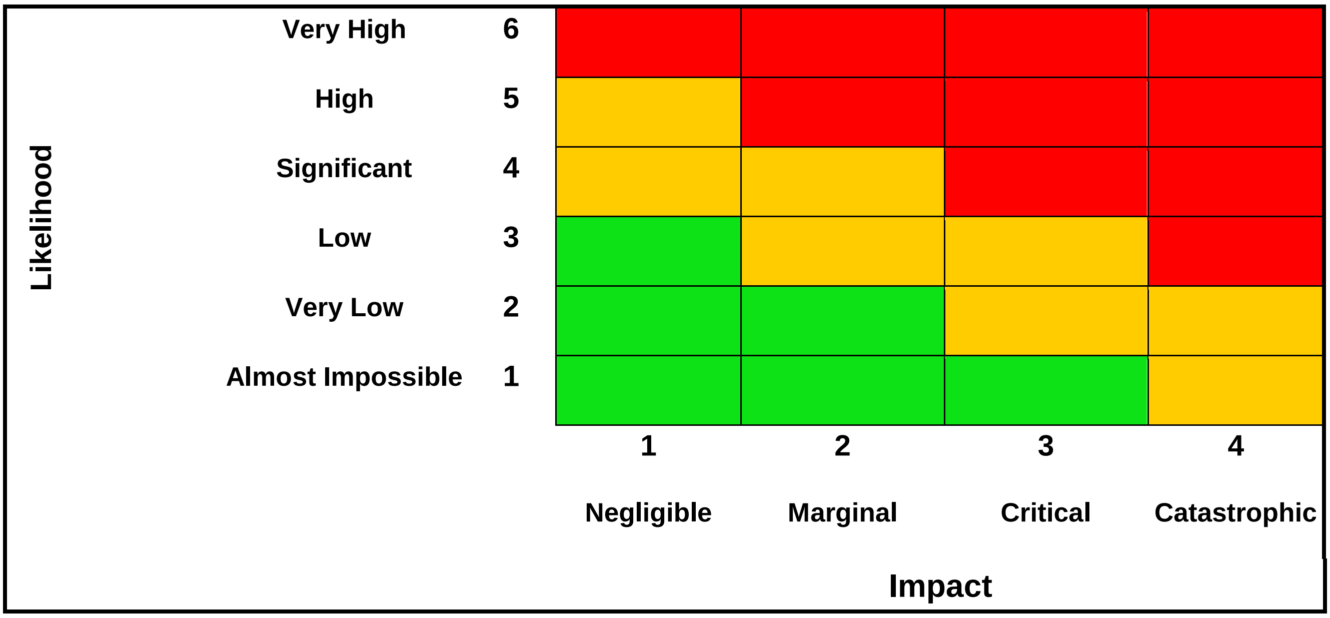
New projects	Making optimal investment decisions / prioritising between projects which are competing for resources	Integral to risk management Option appraisal Opportunity cost
New policies	Policy decisions create expectations where the organisation has uncertainty about delivery	Affordable housing

7. Assessment of Risks

The Council has adopted the following framework for assessing risks to the Council in terms of both likelihood and impact.

Current Risk is defined as the probability and implications of an activity resulting in negative and/or undesirable consequences BEFORE any planned control measures are introduced.

Target Risk is defined level of risk after mitigating actions have been taken to reduce adverse and potentially long-term effects prior to the event occurring.



Risks falling within the red zone are outside the tolerable range of exposure and mitigations must be put in place to reduce the exposure or be referred to a higher managerial level for discussion and decision when they arise.
Risks falling within the amber zone are likely to require some measure of mitigation in order to be acceptable.
All risks falling within the green zone are considered tolerable and unlikely to require further action or mitigation unless circumstances alter.

Risks are ‘graded’ by multiplying the Likelihood by Impact to get the total risk grading, e.g.: Significant (4) x Critical (3) = risk grade 12.

8. Addressing Risk

If the preceding steps are taken the risk will be mitigated to an acceptable level of tolerance. A key part of this will be the need to both contain threats and take advantage of opportunities.

There are four key aspects to addressing risk and internal control:

1.TOLERATE	The exposure may be tolerable without any further action being taken. The ability to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit gained. In these cases, the response may be to tolerate the existing level of risk. This option may be supplemented by contingency planning for handling the impacts that will arise if the risk is realised.	
2.TREAT	By far the greater number of risks will be addressed in this way. The purpose of treatment is that whilst continuing with the activity giving rise to the risk, action (control) is taken to constrain the risk to an acceptable level. Such controls can be further sub-divided according to their particular purpose (see below).	
	PREVENTIVE CONTROLS	Controls designed to limit the possibility of an undesirable outcome. The more important it is that an undesirable outcome should not arise, the more important it becomes to implement appropriate preventive controls. The majority of controls implemented in organisations tend to belong to this category (preventive controls), e.g.: separation of duty whereby no one person has authority to act without consent of another; only those suitably trained and authorised being permitted to handle media enquiries to prevent inappropriate comment being made to the press.
	CORRECTIVE CONTROLS	Controls designed to correct undesirable outcomes which have occurred. They provide a means to achieve some recovery against loss or damage, e.g.: contract terms to allow recovery of an overpayment.
	DIRECTIVE CONTROLS	Controls designed to ensure that a particular outcome is achieved. They are particularly important when it is critical that an undesirable event is avoided, e.g.: Health and Safety, a requirement that protective clothing be worn when undertaking dangerous duties, or that staff be trained with required skills before being allowed to work unsupervised.
	DETECTIVE CONTROLS	These controls are designed to identify occasions of undesirable outcomes having been realised. Their effect is by definition “after the event” so they are only appropriate when it is possible to accept the loss or damage incurred, e.g.: stock or asset checks (which detect whether stocks or assets have been removed without authorisation), reconciliation (which can detect unauthorised transactions), “Post Implementation Reviews” which detect lessons to be learnt from projects for application in future work, and monitoring activities which detect changes that should be responded to.
3.TRANSFER	For some risks the best response may be to transfer them. This might be done by conventional insurance, or by paying a third party to take the risk in another way. This option is particularly good for mitigating financial risks or risks to assets. The transfer of risks may be considered to either reduce the exposure of the organisation or because another organisation (which may be another government organisation) is more capable of effectively managing the risk. It is important to note that some risks are not (fully) transferable - in particular it is generally not possible to transfer reputational risk even if the delivery of a service is contracted out. The relationship with the third party to which the risk is transferred needs to be carefully managed to ensure successful transfer of risk.	
4.TERMINATE	Some risks will only be treatable or containable to acceptable levels by terminating the activity. It should be noted that the option of termination of activities may be severely limited in government when compared to the private sector; a number of activities are conducted in the government sector because the associated risks are so great that there is no other way in which the output or outcome, which is required for the public benefit, can be achieved. This option can be particularly important in project management if it becomes clear that the projected cost / benefit relationship is in jeopardy.	

9. Checklist for identifying risk areas

Use this checklist to help you identify risks for your service area or project associated with each of these factors.

EXTERNAL

Political	☐	**Economic**	☐	**Social**	☐	**Technological**	☐	**Legal**	☐	**Environmental**	☐

OPERATIONAL

Service Failure	☐	**Project delivery**	☐	**Resources**	☐	**Relationships**	☐	**Operations**	☐
Reputation	☐	**Governance**	☐	**Scanning**	☐	**Resilience**	☐	**Security**	☐

CHANGE

Capability	☐	**Transformation programme**	☐	**New projects**	☐	**New policies**	☐

10. Service Area Risk Register

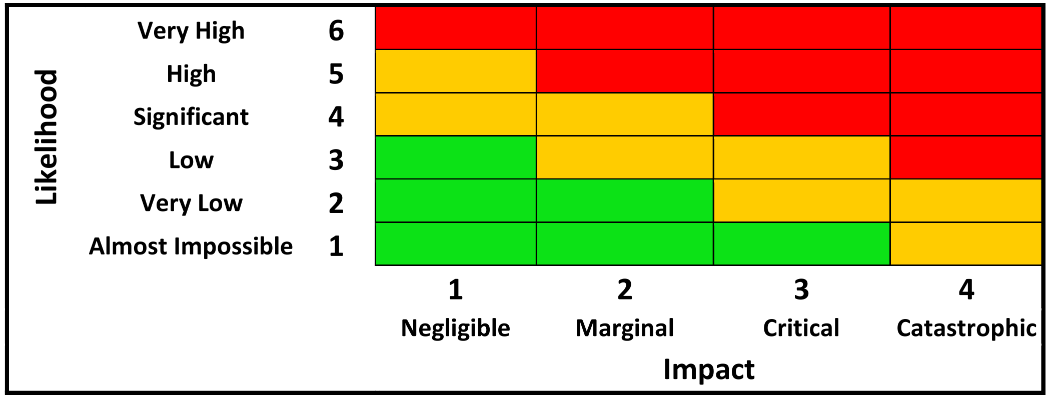
Corporate Risk Matrix/Guide is referenced on the below page to assist with providing the correct risk scoring for the risks you identify. You can also find this on the intranet.

No	Risk Description	Impact	Owner	Current Risk			Planned Control Measures	Timeline	Target Risk (After Mitigation)		
				Likelihood	Impact	Risk grading			Likelihood	Impact	Risk grading

<u>**Examples**</u>	**IMPACT (grade 1 to 4)**			
	1 - Negligible	**2 - Marginal**	**3 - Critical**	**4 - Catastrophic**
Financial impact	£0k - £25k	£25k - £250K	£250K - £2M	£2M+
Service Provision	No effect	Slightly reduced	Service suspended short term/reduced	Service suspended long term Statutory duties not delivered
Health & Safety	Sticking plaster / first aider	Broken bones/Illness	Loss of life/major illness	Major loss of life/large-scale major illness
Objectives		Objectives of one key service area not met	Directorate objectives not met	Corporate objectives not met
Morale		Some hostile relationship / minor non co-operation	Industrial action	Mass staff turnover / unable to attract staff
Reputation	No media attention / minor letters	Adverse local media Leader	Adverse national publicity	Will be remembered for years!!
Government relations		Poor assessment(s)	Service taken over temporarily	Service taken over permanently

LIKELIHOOD (grade 1 to 6)		
	Probability	**Timing**
6 - Very High	> 90%	This week
5 - High	55% to 90%	Next week / this month
4 - Significant	15% to 55%	This year
3 - Low	5% to 15%	Next year
2 - Very Low	1% to 5%	Next year to five years
1 - Almost Impossible	0% to 1%	Next 10 years

Risk Matrix (Corporate)



Note: **Multiply** Likelihood by Impact to get total Risk grading

11. Support

This toolkit is designed to help you identify risks for your service area or project. If you need further support or would like an example to assist, the Business Improvement team are available to provide guidance and advice.

The intranet is also a great source of information: -

- Risk Register Template
- Risk Management Strategy
- Project Management SharePoint