CITY OF
YORK
COUNCIL

Risk Management Guide

City of York Council
Risk Management Guide Contents

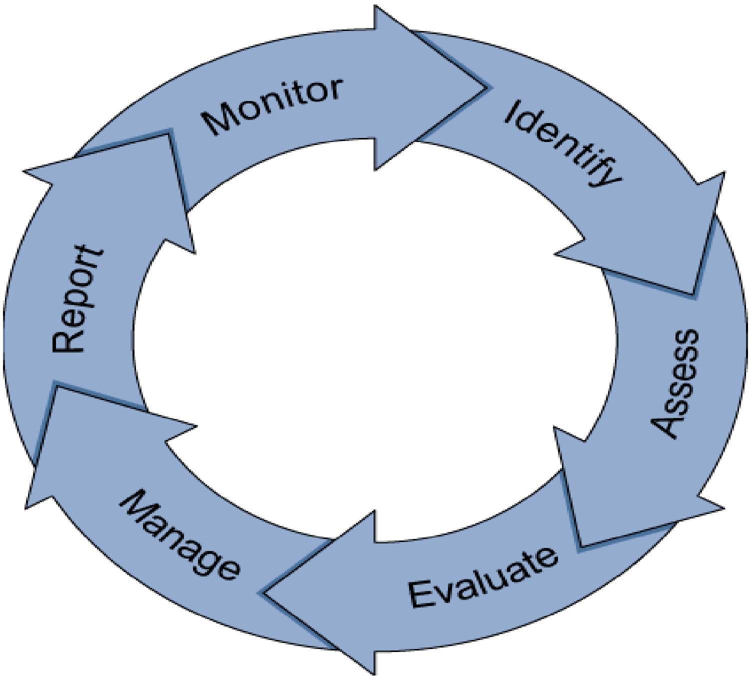
Introduction

1. This document is designed as a guide for all employees, with risk management responsibilities, to explain what to do and what to document at each stage of the risk management cycle.

Risk Management Cycle

2. Exhibit 1 shows the standard risk management cycle adopted by City of York Council.

Exhibit 1.



3. Phases and related activities of the risk management cycle.

Phase		Activity
1.	**Identify**	the risks that exist or could emerge
2.	**Assess**	those risks for their potential impact and likelihood
3.	**Evaluate**	the need for further action
4.	**Manage**	put in place mechanisms to reduce risks
5.	**Report**	significant (high) risks to the appropriate level
6.	**Monitor**	the effectiveness of any risk management action taken

Identify – what to do

4. To ensure all existing and potential risks are identified, it is important to consider how they may arise in the context of the relevant business area.

5. The table below provides a non-exhaustive list of when and how risks can arise and their potential affect on the organisation.

What we do	How risks can arise	What affect they can have
Working in **Partnership** with others	• Poor communication • Ill defined priorities • Lack of commitment • Partners roles not agreed	• Waste resources • Fail to achieve objectives • Increase costs • Negative press coverage
Delivering **Projects** & Programmes	• Possible deviation from the expected or desired outcome	Failure to deliver: - • on time • within budget • to specification
Achieve Corporate Strategy (**Strategic**)	• Conflicts in prioritisation of resources • Lack of commitment • Poor performance	• Negative press coverage • Reduced customer satisfaction • Reputation of organisation
Service delivery (**Operational**)	• Lack of procedures/ controls • Unanticipated changes in external environment	• Reduced customer satisfaction • Poor productivity • Inability to manage customer demand & expectation • Negative press coverage

6. The identification process should involve a combination of a forward-looking (proactive) approach, and a retrospective review of past threats and opportunities.

7. A visioning (identification) session, allows lessons to be learnt from past experiences and ensures future risks are identified, that can be used to shape future plans and actions.

Identify – what to document

8. **Risk Title**

All risks identified as significant should be documented with an appropriate title, which;

- includes a starting descriptor such as: -
  - o Reduction of….
  - o Loss of….
  - o Disruption to….
  - o Inability to….
  - o Increase in….

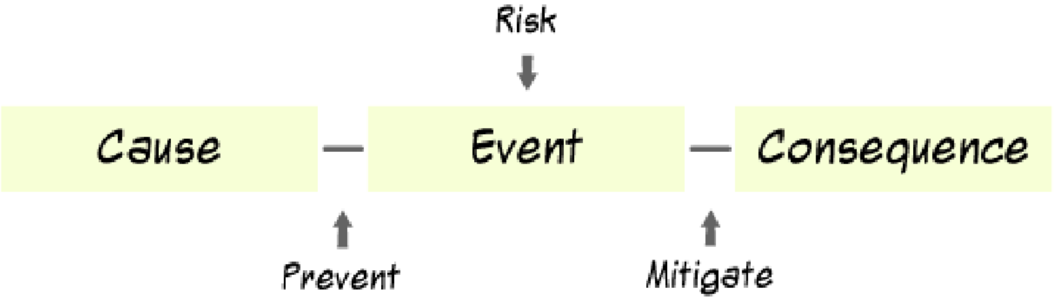
9. **Risk Detail & Implications**

The risk detail and implications should;

- be clear & understandable
- mention the cause and consequence, if possible

Using the "cause – event – consequence" principle helps to describe what the risk event is.

Cause – explains what can lead to the event.
Event – describes what it involves – **this is the risk!**
Consequence – what the effects are on the organisation.



10. **Risk Owner**

The risk owner should be the person who understands the risk, including it's causes and consequences, and where the risk is considered to fall within their remit. This does not necessarily mean that taking action to manage the risk is their sole responsibility and indeed it may well be beyond their scope of authority to implement the necessary controls, however, it will be within the expectations of their role to flag this as a potential risk.

11. **Risk type** select the appropriate business area, Operational, Strategic, Partnership or Project.

12. **Risk Category** select the appropriate category from appendix 1.

Assess – what to do

13. Risk has two elements, the probability of an event occurring (likelihood) and the consequence if it does occur (impact). The aim of risk analysis is to estimate likelihood and impact, this is done at two levels (Gross and Net)

14. **Gross risk rating**

    Also known as the inherent risk. This is the estimation of the impact and likelihood of the risk before the effects of controls are considered. (How severe the risk could be if all mitigating measures were removed).

15. **Controls**

    List the mitigating and preventative measures that are in place to reduce the likelihood and/or the impact of the risk.

    Preventative – help to reduce the likelihood of the event.
    Mitigating – help to lessen the impact of the consequence of the event.

16. **Net risk rating**

    Also known as the residual risk. This is the analysis of the impact and likelihood in the context of existing control measures. (The **current** potential impact and likelihood if the risk materialised)

Assess – what to document

17. **Gross Score** - follow the steps below and see Risk Criteria at appendix 2.

    - Determine the risk's potential impact.
    - Determine the potential likelihood of the risk occurring.

    Using table 1 in Risk Rating Matrix (appendix 3) find the relevant score in the matrix.

18. **Control Title**

    Identify the existing control(s).

19. **Control Owner**

    This is the person responsible for ensuring the implementation and effectiveness of the control. It does not have to be the same as the risk owner.

Assess – what to document (continued)

20. **Control Description**

Give an outline of how the control works to reduce either the likelihood or impact.

21. **Implementation Status**

This is to advise whether the control is: -
Complete, work in progress, not started, time frame planned or on going.

22. **Reduction in Impact and Likelihood**

State whether the control reduces the impact and/or likelihood of the risk.

23. **Review Frequency**

How often is the control reviewed to ensure it is in place and effective – Weekly, monthly, quarterly, bi-annually, annually?

24. **Review Method**

How is the control reviewed to ensure its effectiveness – internal audit, internal review, management reports, self assessment, project board, external consultants or no assurance (this is when there is no review to ensure the effectiveness of the control).

25. **Net Score -** follow the steps below and see Risk Criteria at appendix 2.

- Determine the risk's current potential impact.
- Determine the current likelihood of the risk occurring.
- Using table 1 in Risk Rating Matrix (appendix 3) find the relevant score in the matrix.

Evaluate – what to do

26. The aim of the this phase is to identify the most significant risks facing the Authority, which will put you in a much better position to anticipate problems and take proactive management style if the worst happens. The output should be a prioritised list of risks for further action.

Evaluate – what to document

27. **Conclusion**

Each documented risk should have a conclusion assigned to it.

- **Tolerate** – accept the risk exposure, supplemented by contingency plans if necessary.
- **Treat** – take appropriate action to constrain the risk to an acceptable level or take advantage of the opportunity.
- **Transfer** – for example by insurance or paying a third party to take the risk in another way.
- **Terminate** - terminating the activity giving rise to the risk, where possible, bearing in mind any residual reputational risks that could still exist.

Manage – what to do

28. Identify what actions you want to take to further reduce the risk.

29. Risk action or treatment is the process of planning and taking action to minimise the likelihood of the risk occurring and/or reducing the severity of the impact should it occur. This usually requires the identification and implementation of projects, or revision of service delivery procedures.

30. It is important that they are proportionate to the risk and give reasonable assurance of confining likely consequences. Every action has an associated cost and it is important that it offers value for money in relation to the risk it is managing.

Manage – what to document

31. **Action Title**

Identify the action(s) to be taken.

32. **Action Owner**

Allocate an action owner, who will take responsibility for implementing/ensuring implementation of the course of action.

33. **Priority**

What priority will be given to this action? High, Medium or Low?

34. **Target Date**

What date is this action to be completed by?

35. **Action Detail**

Give an outline of how the action will work to further reduce the likelihood and/or impact.

36. **Target Date**

Determine the date the action is to be completed by.

Report – what to do

Risk Level	Identification	Monitoring		Reporting	Frequency
Corporate	Corporate Management Team	Corporate Management Team	****HIGH LEVEL RISK ESCALATION REPORTING****	Executive Committee	Annually & Ad Hoc
				Audit & Governance Committee	Quarterly
Directorate	Directorate Management Team	Directorate Management Team		Corporate Management Team (CMT)	Quarterly
Division/ Group/ Arm	Service Planning	Management Team		Directorate Management Team (DMT)	Quarterly
Service	Manager	Manager & Team		Management Team	Quarterly
ITD Plan Projects	Project Manager & Leader	Project Board		Corporate IT Strategy Group	Quarterly
Other Projects				CMT or DMT	Ad Hoc
Partnership	Client Officer	Partnership Board		Directorate Management Team	Ad Hoc

**** HIGH LEVEL RISK ESCALATION REPORTING****

significant risks (those evaluated with a net rating of 16 or above) should be reported to the appropriate senior management team

37. Risk exists in all areas and at all levels therefore a robust reporting line to escalate and cascade information is essential.

38. Identify the risks with a net rating of 16 or above and report these to the appropriate senior management team (refer to table).

Report – what to document

39. Ensure that any comments and information made by the management team reviewing the high level risk escalation report are recorded.

Monitor – what to do

40. Risk monitoring is necessary to ensure the effectiveness of the risk management framework, to identify required further action and to flag when risks are changing. Therefore, a process should be put in place to review whether the same risks still exist, new risks have arisen, and whether the level of exposure has changed. This will help to identify significant changes, adjust risk priorities and deliver assurance on the effectiveness of control.

Monitor – what to document

41. Document any changes to the risk as it is described, scored and managed, and make sure you update the next review date.

Next Steps

42. Risk management is an on-going process, and it is important that risks are considered continuously. New risks that were not considered at the outset can emerge at anytime; therefore it is necessary to considered and review your assessment and position.

Appendix 1

Risk Type & Category

Type	Detail
Strategic	Risks concerning medium to long-term goals and objectives of the organisation.
Operational	Risks involved with the specific operational activities of the organisation.
Partnership	Risks arising from partnership activities of the organisation.
Project	Risks emerging from project and programme activities of the organisation.

Ref	Category	Detail
01	**Governance & Management**	Risks arising from the stewardship of the Council including conflicts of interest.
02	**Legal & Regulatory**	Risks arising from failure to comply with laws and regulations.
03	**Health & Safety and Property**	Risks arising from hazards to people and assets.
04	**Financial & Efficiency**	Risks to the council's ability to meet its financial commitments and improve efficiency.
05	**Competition & Procurement**	Risks affecting the competitiveness of the service (cost or quality) and/or its ability to deliver best value.
06	**Stakeholder**	Risks affecting the council's employees and customers.
07	**System & Technology**	Risks include changes in pace and scale of customer demands and reliance on ITT.
08	**External**	Risks arising from changes to the world outside the organisation's control: political, economic, social, technological, legal and environmental.
09	**Data Quality**	The risk arising out of the use of inaccurate and poor quality data.
10	**Reputational**	Risks affecting the reputation of the council.

Appendix 2

Risk Assessment Criteria –**Impact**

	Financial Impact	Compliance & Regulation Impact	Local Community or Target Customer Base	Authority Reputation	Health & Safety
Catastrophic	**> 25% of budget**	**Action in national court. Imprisonment of employees**	**>25% affected**	**National media coverage**	**Fatal injury**
Major	**10-25% of budget**	**Action in national court. Major fine**	**Larger group affected (10-25%) or smaller group for more than 6 months**	**National media coverage**	**Multiple serious injury**
Moderate	**5-10% of budget**	**Action in local court. Substantive fine**	**Larger percentage affected (5-10%) or small % for 3-6 months**	**Local media coverage**	**Serious injury**
Minor	**2-5% of budget**	**Local restrictions or minor fine**	**Limited to a small percentage (<5%) and for a short duration (< 3 months)**	**Little or no media coverage**	**Multiple minor injury**
Insignificant	**<2% of budget**	**Notification of non-compliance but no further action**	**Little impact outside the Council itself**	**Little impact outside the Council itself**	**Minor injuries**

Risk Assessment Criteria – **Likelihood**

Highly Probable	**More likely to occur or will occur more often**
Probable	⬇
Possible	
Unlikely	
Remote	**Less likely to occur or will occur less often**

Appendix 3

Risk Rating Matrix

Table 1

Impact

Catastrophic	**17**	**22**	**23**	**24**	**25**
Major	**12**	**18**	**19**	**20**	**21**
Moderate	**6**	**13**	**14**	**15**	**16**
Minor	**2**	**8**	**9**	**10**	**11**
Insignificant	**1**	**3**	**4**	**5**	**7**
	Remote	Unlikely	Possible	Probable	Highly Probable

Likelihood

Risk Evaluation Table

Table 2

Colour	Score	Assessment	Required Action
🟦	1 – 5	**Very Low** (tolerate)	Periodic passive monitoring
🟩	6 – 10	**Low** (tolerate)	Regular monitoring
🟨	11 – 15	**Medium** (tolerate)	Frequent monitoring
🟧	16 – 20	**High** (treat)	Constant monitoring, action plan and measures to be put in place to reduce exposure
🟥	21 – 25	**Critical** (treat)	Requires immediate action

Appendix 4

Risk Management Terminology General

Term	Definition
Risk	combination of the likelihood (probability) of an event and its impact (consequence)
Impact	outcome of an event, its consequence & business impact
Likelihood	extent to which an event is likely to occur (probability)
Event	occurrence of a particular set of circumstances (risk)
Cause or source (aka hazard)	item or activity having potential for a consequence (in the context of health & safety, source is a hazard)
Risk criteria	terms of reference by which the significance of a risk is assessed
Risk Management	coordinated activities to direct and control an organisation with regard to risk
Risk Management system	set of elements of an organisation’s management system concerned with managing risk

Risk Assessment

Term	Definition
Risk assessment	process of risk analysis at gross & net level
Risk analysis	systematic use of information to identify sources and to estimate the risk
Risk identification	process to find, list and characterise elements of risk
Source identification	process to find, list and characterise sources (causes)
Risk evaluation	process of comparing the estimated risk against given risk criteria to determine the significance of the risk

People & Organisational Terms

Term	Definition
Stakeholder	any individual, group or organisation that can affect, be affected by, or perceive itself to be affected by, a risk
Interested party	person or group having an interest in the performance or success of an organisation
Risk perception	way in which a stakeholder views a risk, based on a set of value or concerns
Risk communication	exchange or sharing of information about risk between the decision maker and other stakeholders

Risk Treatment & Control Terms

Term	Definition
Risk treatment	process of selection and implementation of measures to modify risk
Risk control	action of implementing risk management
Risk optimisation	process, related to a risk to minimise the negative and maximise the positive consequences and their respective likelihood
Risk reduction	actions taken to lessen the likelihood, negative impact or both, associated with a risk
Mitigation	limitation of any negative impact of a particular event
Risk avoidance	decision not to become involved in, or action to withdraw from, a risk situation
Risk transfer	sharing with another party the burden of loss or benefit of gain from a risk
Risk financing	provision of funds to meet the cost of implementing risk treatment and related costs
Risk retention	acceptance of the burden of loss, or benefit of gain, from a risk
Risk acceptance	decision to accept exposure to a risk
Inherent risk	exposure to a risk before treatment (gross risk)
Residual risk	remaining exposure to a risk after treatment (net risk)