

Appendix 2

RISK MANAGEMENT TOOLKIT

Stage 1: Identify the risk

- Consider the 14 categories of risk
- Discuss with colleagues and group
- Examine trends
- Analyse previous problems
- Consider experiences from other organisations

Risk Category	Description Category of Risk	Strategic or Service
Political	Incorrect strategic priorities – not meeting government agenda – failure to make decisions quickly – decision made using incomplete or faulty data – failure to fulfil commitments – community planning oversights or errors.	Strategic (Reputation / Legal)
Economic	National or regional economic problems – failure to control capital – treasury risk – failure to identify business and /or service opportunities.	Strategic (Financial)
Social	Failure to meet the needs of disadvantaged communities – impact of demographic changes – failure to address employment challenges – lack of development – failure of partnership working – failure in delivering life-long learning – failure to control crime and disorder – failure to control civil unrest.	Strategic (Financial / Legal)
Legislative	Judicial review – HRA breaches – failure to adequately respond to new legislation – intervention by regulatory bodies.	Strategic (Financial / Legal)
Competitive	Loss of service to central government, agencies and private sector – failure to demonstrate best value – failure of bids for government funds.	Strategic (Financial)
Customer	Failure to undertake appropriate consultation – impact of social policies – poor public and media relations.	Strategic (Reputational)
Technological	Strategic: Obsolescence of technology – inadequate implementation of security policies leading to disclosure, modification or loss of data – failure of communications systems	Strategic & Service (Financial / Reputation / Technological)
Technological	Service: Failure of large technology-related project – failure of critical IT systems affecting service delivery – breach of security of network or data – mismanagement of internet and/or intranet.	Strategic & Service (Financial / Reputation / Technological)
Environmental	Impact on recognised environmental policies – noise, contamination and pollution – impact on planning and transportation policies.	Strategic & Service (Reputation / Legal)
Professional	Failure to recruit or retain qualified staff – lack of training – overreliance on key officers – inefficient or ineffective management processes – inability to implement change – lack of staff motivation or efficiency – bad management of partnership working.	Service (Financial / Reputation)
Financial	Failure of major project – failure to prioritise, allocate and monitor budgets – inefficient or ineffective processing of financial documentation.	Service (Financial / Reputation / Legal)
Legal	Failure to meet statutory duties and /or deadlines – disclosure of DPA related data – failure to comply with Central Government directives on procurement of works, supplies and services – failure to implement legislative changes.	Service (Legal)
Physical	Attacks on personnel – loss of personnel – loss of intangible assets – non-compliance with H&S legislation – loss of physical assets.	Service (Personnel/Asset)
Partnership / Contractual	Over-reliance on suppliers or contractors – failure of outsource provider to deliver – failure in standards in quality – non-compliance with procurement policies.	Service (Financial / Reputation / Legal)
Information	Systems and management data not up-to-date – ineffective prediction of trends and forecasting service needs.	Service (Financial / Technology)

Stage 2: Assess the risk

Threats	Consider events or situations that could exploit or trigger known or unknown vulnerabilities. (Threats are generally Natural, Human or Environmental)			
Vulnerabilities	Consider weaknesses in control, either identified or perceived, that could allow the threat to be realised.			
Risks	Where there is a threat that can be realised through a vulnerability, this should be considered as a risk and			
	recorded.			

Stage 3: Rate the risk

Consider the **probability** of the event happening over a period of time. Consider the **impact** on the Authority of an event being realised.

PROBABILITY x IMPACT + RISK RATING

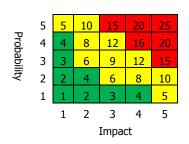
PROBABILITY

Descriptor	Level	Probability of the event happening over the period of one year
Probable	5	≥ 90%
Likely	4	≥ 50% and < 89%
Possible	3	≥ 20% and < 49%
Unlikely	2	≥ 1% and < 19%
V. Unlikely	1	< 1%

IMPACT ON THE AUTHORITY OF AN EVENT BEING REALISED

Descriptor	Level	Financial	Reputation	Legal	Personnel	Asset	Technology
Severe	5	≥£1M	Irrecoverable	Major legal or regulatory sanction	Death	Massive irrecoverable damage / total loss	No alternative manual fall- back
Significant	4	≥ £250K	Legally damaging (civil or criminal)	Significant legal or regulatory sanction	Permanent avoidable disability	Major damage / significant loss	Manual fall- back available in the short term
Moderate	3	≥£50K	Perception	Some legal or regulatory sanction	Sever injury / hospitalisation	Moderate damage	Manual fall- back available in the medium term
Minor	2	≥ £25K	Mildly embarrassing	Some legal or regulatory notification	First Aid required	Minor damage	Manual fall- back available in the long term
Insignificant	1	≥ 1K	None	No legal or regulatory consequences	None	None	Manual fall- back available indefinitely

RISK RATING MATRIX



RISK RATING DEFINITIONS

Risk Rating	Level of Risk	Action required to mitigate risk
≥ 15	HIGH	Immediate action required to transfer, treat or remove the risk
≥ 5 and <15	MEDIUM	Some degree of planned action required to transfer, treat, tolerate or remove the risk
< 5	LOW	No further action required – continue monitoring the situation

Stage 4 : Control the risk

Assess the current controls in place to establish whether they are Effective, Partially Effective or Ineffective.

Develop SMART actions to control the risk by:

- Transferring the risk
- Treating the risk
- · Tolerating the risk
- Removing the risk

Any Service risks that are HIGH or any common risks that could aggregate into a Strategic Risk must be escalated to JLT for review.

Stage 5: Monitor the risk

Risks should be regularly reviewed and reported through:

- Strategic Risk Register Group meetings
- JLT meetings
- Head of Service and Service Managers meetings
- Performance, Audit & Scrutiny Committee meetings

Risk ratings and relevance must be reassessed regularly or whenever a trigger event occurs, such as:

- Risk scenario changes
- A new risk is identified
- There is a significant change in working practice, environment or system