Stage 1: Identify the risk

- Consider the 13 categories of risk (as per UK Gov Orange Book 2023)
- Discuss with colleagues and group
- Examine trends
- Analyse previous problems
- Consider experiences from other organisations

Risk Category	Description Category of Risk
Strategy	Risks arising from identifying and pursuing a strategy, which is poorly defined, is based on flawed or inaccurate data or fails to support the delivery of commitments, plans or objectives due to a changing macro-environment (e.g. political, economic, social, technological, environment and legislative change).
Governance	Risks arising from unclear plans, priorities, authorities and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance.
Operations	Risks arising from inadequate, poorly designed or ineffective/inefficient internal processes resulting in fraud, error, impaired customer service (quality and/or quantity of service), non-compliance and/or poor value for money.
Legal	Risks arising from a defective transaction, a claim being made (including a defence to a claim or a counterclaim) or some other legal event occurring that results in a liability or other loss, or a failure to take appropriate measures to meet legal or regulatory requirements or to protect assets.
Property	Risks arising from property deficiencies or poorly designed or ineffective/inefficient safety management resulting in non-compliance and/or harm and suffering to employees, contractors, service users or the public.
Financial	Risks arising from not managing finances in accordance with requirements and financial constraints resulting in poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting.
Commercial	Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, and/or failure to meet business requirements/objectives.
People	Risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviours, the unavailability of sufficient capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance.
Technology	Risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience.
Information	Risks arising from a failure to produce robust, suitable and appropriate data/information and to exploit data/information to its full potential.
Security	Risks arising from a failure to prevent unauthorised and/or inappropriate access to the estate and information, including cyber security and non-compliance with General Data Protection Regulation requirements.
Project/Programme	Risks that change programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits to time, cost and quality.
Reputational	Risks arising from adverse events, including ethical violations, a lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, leading to damages to reputation and or destruction of trust and relations.

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 for planning for 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	Perception	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

Probability					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

1 2 3 4 5

Impact

RISK RATING DEFINITIONS

Risk Rating	Level of Risk	Action required to mitigate risk
≥ 15	**HIGH**	**Immediate action required** to transfer, treat, tolerate 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 the Strategic Risk Register Group for review.

Stage 5: Monitor the risk

Risks should be regularly reviewed and reported through:

- Strategic Risk Register Group 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