A. AI Risks

Risk Details

There is the risk of unauthorised use of generative AI, dependency on third-party platforms, heightened threat of Cyber attacks inadequate cyber security controls, and weak information governance could lead to reputational damage, resident mistrust, operational disruption, data breaches, and regulatory penalties.

Risk Update

In early 2025, Internal Audit initiated a governance review to understand whether the organisation had the strategy, controls and capability needed to support safe, ethical and compliant adoption. The review was prompted by concerns that AI activity was outpacing the Council’s maturity and that existing risk, procurement and data protection processes were not designed with AI-specific risks in mind.

The review concluded in October 2025 with a Limited Assurance rating, identifying gaps in policy, governance, training, procurement and ongoing monitoring. These issues stem from several underlying drivers: the speed and decentralisation of AI adoption, the absence of an AI Strategy, early-stage governance maturity, limited staff capability, insufficient vendor assurance processes, and the rapidly evolving regulatory environment.

In December 2025, the Directors’ Risk Review recommended elevation of AI to the Strategic Risk Register, recognising that the combination of uncoordinated adoption, compliance risk and organisational exposure constituted a material corporate-level threat. The risk was formally added in January 2026.

The core risk arises from AI adoption outpacing the Council’s governance maturity, leading to inconsistent standards, gaps in oversight, and uneven capability across services. Key contributing factors include the absence of a cohesive AI Strategy, incomplete policy framework, early-stage staff literacy, insufficient vendor assurance arrangements, and emerging regulatory obligations under UK GDPR, transparency requirements, and evolving UK/EU AI standards.

The council is addressing these risks as work over 2025/26 has focused on establishing stronger governance foundations for AI activity across the organisation. Although Brent’s AI maturity remains in its early stages, important controls are already in place to reduce exposure and create a clearer framework for responsible adoption. A strengthened governance model now provides oversight across strategy, ethics, data protection and cyber security. The Programme Manager for AI & Automation has taken responsibility for leading delivery of the Council’s AI strategy. Brent also incorporates national best practice by adopting guidance from the Government Digital Service (GDS) and the Local Government Association (LGA), ensuring its frameworks, ethical safeguards, and delivery models remain consistent with sector-wide standards

Risk Scores	I	L	T	Trend
CURRENT	**4**	**3**	**12**	↔
Previous	4	3	12	
Target	3	2	6	

▪ Key Controls & Mitigating Actions

- We have an AI and Data Board, supported by a dedicated Data Ethics Board, to provide expert guidance on the responsible development and deployment of AI systems.
- Clear accountability held by the Director of CII, who is responsible for ensuring AI activities across the organisation meet regulatory, ethical, and organisational expectations.
- Strategic oversight provided by the Programme Manager for AI & Automation, ensuring coordinated delivery, risk management, and alignment across all AI initiatives. This role acts as the central governance lead, ensuring projects follow agreed standards and frameworks.
- Shadow Ai Monitoring is now in place to detect and manage unauthorised Ai use.
- Mandatory completion of DPIAs and AI Impact Assessments for all AI projects to ensure potential risks, especially around data protection, bias, and individual rights. And shadow AI monitoring.
- Corporate Risk monitoring to track AI-related risks at an organisational level, ensuring they are visible, assessed, and managed through established risk-management processes. This provides ongoing oversight as systems evolve.
- Cyber assurance provided through the STS team, to identify vulnerabilities and reduce the risk of AI-enabled cyberattacks. This ensures AI systems meet high security standards before going live

AI Risks

♦ Action Plan

Ref	Action	Target Date	Status	Comments
1.	We will Develop AI Strategy & Policy Framework	31 July 2026	In Progress	A Council wide AI strategy is being drafted, supported by a comprehensive AI Policy Framework. This will set out minimum standards for transparency, data use, ethical safeguards, and assurance requirements. This work directly supports the creation of a consistent governance baseline across the organisation.
2.	We will Strengthen governance structures and KPIs	31 July 2026	In Progress	Governance mapping has been completed and will inform a strengthened structure including clearer decision rights, reporting lines, and KPIs. This forms a core part of the long-term capability building programme and supports the move from High to Medium risk.
3.	Introduce risk based, Responsible and Ethical AI training for Brent Staff	31 July 2026	In Progress	A new mandatory training framework is being developed to improve cultural readiness and ensure staff understand safe use expectations, risk indicators, escalation routes, and ethical considerations. This will become a baseline requirement for all AI related activity.
4	Update procurement & supplier due diligence	31 July 2026	Planned	Procurement and due diligence processes will be updated to incorporate AI specific requirements, including transparency obligations, model governance expectations, data protection compliance, and risk disclosures. This ensures suppliers meet minimum AI safety standards.
5	Identify AI vendors appropriate to our tooling strategy and explore internal AI capability	31 July 2026	In progress	A catalogue of AI vendors and tools in use across Brent is being developed. This will support risk management, contract visibility and alignment to the Council’s tooling strategy. Internal capabilities will also be assessed to ensure we can safely build and manage AI in house where appropriate.

Risk Evaluation Matrix

The following impact and likelihood criteria are used to analyse and evaluate the Council's Strategic Risks.

IMPACT

Score	Financial	Service Delivery	Health and Wellbeing	Reputation
5	*Major Financial loss (above £2m)*	*Major disruption to a number of critical services*	*Multiple deaths / serious life-changing injuries / extreme safeguarding concerns.*	*Long term damage – e.g. adverse national publicity.*
4	*Significant Financial loss (above £1m)*	*Major disruption to a critical service.*	*Multiple casualties with life changing injuries / significant safeguarding concerns.*	*Medium to long term damage – e.g. adverse local publicity.*
3	*Moderate Financial Loss (less than £1m)*	*Moderate disruption to a critical service*	*Moderate risk of injury / noticeable safeguarding risks.*	*Medium term damage*
2	*Small Financial loss (less than £500k)*	*Moderate disruption to an important service.*	*Low level injuries / safeguarding risks.*	*Short term damage*
1	*Minor financial loss (less than £100k)*	*Brief disruption to important service*	*No immediate impacts to health or wellbeing*	*Some damage to specific functions*

1	2	3	4	5
Rare	**Unlikely**	**Possible**	**Likely**	**Very Likely**
Highly unlikely, but it may occur in exceptional circumstances.	Not expected, but there's a small possibility it may occur at some point.	This event might occur at some point and/or there is a history of occurrence of this risk at this, or other, Councils	There is a strong possibility this event will occur.	This event is expected to occur in most circumstances.

LIKELIHOOD