IDENTIFIED RISK/RISK ACTION PLAN – SRR 4.3

SECTION A – Risk description and existing controls

Risk description	**Data not appropriately managed or effectively used**
Risk theme	Technological
Risk reference	SRR 4.3
Risk owner (name and role)	Kamal Adatia, City Barrister Andrew Shilliam, Director of Corporate Services
Current risk score	9
Response strategy/action	Treat
Target risk score	6
Risk review date	Ongoing - aligned to NCS '10 Steps to Cyber Security' framework, DDaT Target Operating Model (TOM) and in addition considered as part of 1:1s with Chief Digital, Data and Technology Officer on a monthly basis and through regular meetings of the Digital, Data and Technology Board

Potential Impact/Likelihood

Provide a brief summary of the risk that you have identified in this section and the likely impact on the organisation's objectives if the risk occurs.

Council services do not recognise or understand the importance of data that they hold which leads to governance, access, classification, ROPA, and ownership issues. More specifically, it manifests itself in the following ways:

- Failure to safeguard confidential and sensitive data from loss.
- Inability to use data effectively to support decisions.
- Reasonableness / effective management of data.
- Failure to protect data from theft.
- Lack of understanding of data assets and data owners within Services.

Provide a brief explanation of impact of this risk and the why the likelihood is scored as it is (will help with root cause and possible controls)

Potential for litigation and financial loss.
Reputational damage.
Loss of public confidence.
Poor targeting of scarce resources and poorer quality decisions.
Non-compliance with legislation.
Potentially complicated classifying data and identifying data owners.
We aren't able to maximise the opportunities of data utilisation because we don't understand it enough.

Existing action/controls already in place

Describe the specific actions and controls that are already in place now to manage the risk

1. Clear information governance policies, procedures and staff training.
2. Monitoring and reporting of information security incidents and annual reporting on information governance including to Governance and Audit Committee.
3. Corporate Information Group ensures robust policies, procedures and approaches are in place for information management and governance, most recently approving a policy in relation to use of AI tools
4. Key roles including Enterprise Data Architect supporting data collection, storage, management and use.
5. Open data publication via open data platform with clear governance and protocols.

Current risk score with existing measures

Impact	Likelihood	Risk rating (I X L)
3	3	9

Response strategy: Treat

Further management action/controls:

List the further action(s) that will be taken in addition to existing controls to manage the risk. Complete the action plan in section B:

1. Development of a data practitioners' network to continue to improve the sharing and use of data across the Council.
2. DDaT 5 Platforms programme to develop enabling technology platforms around data and reporting and analytics.
3. Undertake an exercise to classify data and identify data owners.

Target risk score with further management actions/controls

Impact	Likelihood	Risk rating (I X L)
3	2	6

SECTION B – Risk action plan

Action No	Control / Action	Action owner	Target date for implementation	Resources/costs required to implement	Progress update - date action completed / pending (if so why)	Success criteria
1	Development of a data practitioners network to continue to improve the sharing and use of data across the Council	Andrew Shilliam	Further embedding and development of the network during 2025	Officer time	March 2025 – update required.	Internal data practitioners working together to continue to drive the organisational culture around data and insights
2	DDaT CRM and integration hub programme to develop enabling technology platforms around data and reporting and analytics	Andrew Shilliam / Carl Skidmore	Ongoing	Officer time Support from partners DLUHC funding to support initial implementation.	2024 – ongoing work on use cases relating to data and insights and development of enterprise data model 2025 – Further work awaits approval of the 5 Platforms programme.	Enterprise-wide architecture which supports effective data management, analytics and insight. Democratises data to reduce duplication, inconsistent records and increase usability of currently siloed data. i.e. “Tell us once, store once and use many”.
3	Undertake an exercise to classify data and identify data owners.	Andrew Shilliam/Kamal Adatia	Ongoing	Officer time		Ensures clear definition between critical and non-critical data.

						Allowing appropriate and cost-efficient data storage, controls and security to be implemented based on criticality of data. Improves capability to respond to cyber attack and data breach by demonstrating understanding and control of data.