

**20 February 2024**

**Risk management update – Strategic Risk Register and Strategic Risks 8 & 9**

**Ward(s):** All

**Portfolios:** All

**Purpose:** For Review

**1. Aim**

This purpose of this report is to provide Audit Committee with the updated Strategic Risk Register (SRR) and provide further detail on Risks 8 and 9 in accordance with the Committee's work programme.

**2. Summary**

2.1 Recent risk management activity has been carried out to refresh the SRR and ensure it contains the most current risks facing the council.

2.2 Finance worked with Executive Directors and Directors from across the council to update the risks, controls and assurances in place. Directorate Risk Registers (DRR's) and the SRR were reviewed by Directors Group and the Corporate Management (CMT) and both confirm that the SRR (and DRR's) adequately reflect the risks facing the council to delivery of its strategic objectives.

**3. Recommendations**

3.1 That Audit Committee note and comment on the updated Strategic Risk Register (SRR), as set out at Appendix 1.

3.1 That Audit Committee receive and comment on Risks 8 and 9 in the context of Appendix 2.

**4. Report detail - Know**

4.1 The role of Audit Committee in relation to risk management is to:

- Monitor the effective development and operation of risk management in the Council;
- Monitor progress in addressing risk related issues reported to the Committee.

This report seeks to provide an updated SRR including the controls associated with the risks to allow Audit Committee to discharge their role.

4.2 Directors reviewed the Directorate Risk Registers (DRR's) and SRR in January 2024 and were asked to consider changes to existing risks, new or common themes within DRR'S and advise those which may require escalation for discussion at CMT. CMT reviewed the SRR at their meeting on 18<sup>th</sup> December 2023. Feedback and changes have been reflected in this report and both Directors and CMT confirm that the SRR (and DRR's) adequately reflect the risks facing the council.

## Directorate Risk Registers and Impact on SRR

- 4.3 All DRR's have been reviewed with a number of completed actions, changes to controls and changes in scores, both upwards and down. A summary of DRR updates for each Directorate is set out below, with the following changes since the last report:

### Adult Social Care, Public Health and The Hub

**Risk 27:** *Compliance with the Equalities Act.* Score reduced from 9 to 6.

**New Risk – Risk 28:** *Programme delivery risk linked with current Public Health cost pressures for 2024/25 onwards.*

### Children's Services

No changes to scores during this quarter, however mitigating/future actions have been reviewed and updated.

### Customer Engagement

No material changes during this quarter.

### EE&C

The following risk has been removed:

Risk 16: *Forced temporary closure of museum (staff shortage / Covid-19)*

### R&T

**Risk 2:** *Low levels of resilience within services (and of critical business knowledge) and capacity to support change / transformation.*

Amendments to existing and future controls.

**Risk 3:** *A significant breach of information / Data / internet security and financial and reputational impact.*

Amendments to existing and future controls.

**Risk 5:** *Insufficient time by key staff dedicated towards horizon scanning, service change and joint partnership working that's capable of maximising opportunities.*

Amendments to existing and future controls.

**Risk 9:** *Payments Replacement Project.* Score reduced from 12 to 9.

- 4.4 There are no implications in relation to the DRR's that required escalating to CMT or Audit Committee for consideration in respect of the SRR.

### Strategic Risk Register updates (compared to September 2023)

- 4.5 Strategic risks are reviewed on a six monthly basis, and as at December 2023 all strategic risks have had their existing controls and future actions reviewed, with a summary of the updates to the risks set out in the table below. All risks have had their existing controls and future actions reviewed and updated where necessary. There have been no changes to the overall risk scores since the last review. The updated risks are attached at Appendix 1 and the table overleaf summarises the position.

Risk	Risk Description	Lead Directorate	Impact	Likelihood	Updated "current" score	Trend	"Target" score
1	Threats to the Economic Growth of Walsall are not identified and mitigated, together with opportunities for sustainable growth being missed.	Executive Director, EE&C	4	4	16	↔	9
2	The Proud Programme does not achieve the outcomes and benefits required to ensure that available resources are directed to deliver the greatest outcomes for the community.	Executive Director, R&T	4	3	12	↔	8
3	Partnership relationships with other sectors and our major suppliers fail to deliver on shared objectives and therefore outcomes for the community.	Executive Director, EE&C	4	3	12	↔	8
4a	The Council is unable to maintain statutory service standards to support the most vulnerable in society.	Executive Director, Children's Services	3	3	9	↔	9
4b	Adult Social Care risk of being unable to maintain service standards to support the most vulnerable in society is ongoing.	Executive Director, ASC	4	4	9	↔	8
5	External Changes in Political and/or legislative environment including ongoing impact of Covid-19.	Executive Director, R&T	3	2	6	↔	6
6	There is a lack of community cohesion and resilience placing increased pressure on public sector resources.	Executive Director, EE&C	4	2	8	↔	4
7	Financial Resilience of the council is impacted by the failure to achieve the savings required or manage demand pressures to enable a balanced budget and Medium-Term Financial Plan to be delivered.	Executive Director, R&T	4	4	16	↔	9
8	Risk of Cyber Security attacks.	Executive Director, R&T	5	3	15	↔	9

Risk	Risk Description	Lead Directorate	Impact	Likelihood	Updated "current" score	Trend	"Target" score
9	Threats in relation to failing to comply with the legal obligations and duties of the UK General Data Protection Regulations, the Data Protection Act 2018 and relevant legislative requirements.	Executive Director, R&T	4	4	16	↔	9
10	Failure to deliver key services in the event of significant business interruption, including services delivered by contractors and partners.	Executive Director, EE&C	4	3	12	↔	8
11	Climate Change - Failure to achieve climate change objectives.	Executive Director, EE&C	4	4	16	↔	12
12	Significant Failure of Governance – a breakdown in governance to merit formal external intervention either from auditors or central government.	Executive Director, R&T	4	2	8	↔	6

4.6 In April 2023 Audit Committee identified four strategic risks that it would like included within their 2023/24 work programme to review. The risks and dates they are being considered by Audit Committee are as follows:

- Risk 2 – considered on 20 November 2023
- Risk 4b – considered on 26 September 2023
- Risks 8 & 9 – 20 February 2024

4.7 Risks 8 and 9 - appendix 2 provides further information on the risk and controls in place and the lead officer has been invited to this meeting to present the report. SRR8 and SRR9 are owned by the Executive Director of Resources and managed within Transformation and Digital; SRR8 is managed by Sharon Worrall, Digital and Technology Services (DaTS) Head of Digital and Operations and SRR9 is managed by Paul Withers, Data Protection Manager Information Governance (IG).

4.8 Both risks are regularly reviewed to ensure that the controls are adequate and mitigating actions are implemented. SRR8 is subject to quarterly Corporate Management Team (CMT) updates and also regular Cyber Security Audits. SRR9 is also reviewed on a regular basis via the forum for information governance board (FIGA) and forms part of a regular Corporate Management Team (CMT) update on the status of compliance and data breaches.

4.9 Further detail is in the table and section below.

Risk	Risk Description	Lead Directorate	Updated "current" score	Previous "current" score	Trend
8	<p>With the council's increasing reliance on digital service delivery if the council is affected by a cyber-attack which would necessitate IT services being withdrawn whilst remedial work is undertaken to restore systems, then it could have a detrimental impact on our ability to deliver some or all services including : support for vulnerable adults and children, ability to contact the council, customer self-serve capability via web and contact centre, impact on financial income and council reputation.</p>	R&T	15	15	↔
9	<p>Threats in relation to failing to comply with the legal obligations and duties of the UK General Data Protection Regulations, the Data Protection Act 2018 and relevant legislative requirements.</p> <ul style="list-style-type: none"> <li>• The inappropriate and or unlawful collection, processing, sharing and retention of information with regards to: <ul style="list-style-type: none"> <li>- New processing or sharing arrangements or systems implementation without assurances or risk assessments</li> <li>- Inappropriate or non-compliant records management practices</li> <li>- Inappropriate sharing of information through new ways of working</li> </ul> </li> <li>• The loss, disclosure or unavailability of information through cyber-attacks</li> <li>• The excessive collection, use, retention or sharing of data</li> <li>• Failing to apply adequate and or appropriate technical or organisational security controls</li> <li>• Failing to comply with the principles in law</li> <li>• Failing to share lessons learnt</li> </ul>	R&T	16	16	↔

<ul style="list-style-type: none"> <li>• Failing to provide sufficient resources to comply with the legal obligations</li> <li>• Failing to provide sufficient funding to enable appropriate levels of security, accountability, compliance and assurance</li> <li>• Failing to comply with recommendations made by the DPO/SRO where risks have been identified</li> <li>• Failing to comply with or abide by policy, procedures, standards and or guidance implemented to support our compliance requirements</li> </ul>				
--	--	--	--	--

**SRR8**

4.10 In managing the Risk SRR8 the existing multi layered controls in place are continuing to protect the Council from Cyber Security attacks however this is an ever-changing landscape with new threats emerging on an almost hourly basis. DaTS has a small, dedicated team which focuses on the detection and prevention of cyber-attacks. A considerable amount of work has been undertaken to maintain and improve Walsall Council’s cyber security posture:

- a strong password regime has been implemented;
- multifactor authentication is now mandatory for all users;
- user accounts not accessed within 30 days are automatically disabled and subsequently deleted;
- the cyber team practice simulated response to threats;
- two simulated data centre failure/cyber-attack exercises were carried out during 2023;
- Moving forward into 2024, CMT have given approval for a simulation exercise to be carried out on an annual basis during business hours;
- Cyber Security training is mandatory for employees and Elected Members and is refreshed on an annual basis;
- Business Continuity Plans and Business Impact Assessments are in place for all services.

4.11 The Cyber Team successfully applied for a grant from Department of Levelling Up, Housing and Communities (DLUHC); this funding was provided along with a Cyber Treatment Plan. The Cyber Treatment Plan highlights 6 areas where improvements can be implemented along with a priority; in total there are 34 individual activities across these 6 focus areas, which the Cyber Team is working on:

<b>Area</b>	<b>Priority</b>
Back-up and Restore	High
Active Directory	Medium
Operating System	Medium
Multi Factor Authentication	Low
Logs	Low
PSN Health Check	Low

DLUHC monitor our implementation progress on a quarterly basis.

4.12 Implementing elements of the Cyber Treatment Plan has seen our Microsoft Secure score (a measure of the level of maturity an organisation has with regards to preparedness for a cyber incident) increase to above 80% - this is 39% higher than that of similar organisations (similar being organisations which are similar in size and partake of the same Microsoft services). The latest Cyber Security Audit (May 2022) gave a rating of Moderate Assurance with regard to Adequacy of System Design and Effectiveness of Operating Controls. The 3 significant recommendations and 8 housekeeping recommendations highlighted in this Audit have been addressed.

<b>Moderate Assurance:</b>	Some improvements are required to enhance the adequacy of the framework of governance, risk management and control.	There is evidence that the level of non-compliance with some of the control processes may put some of the Organisation's objectives at risk.
----------------------------	---	--

### SRR9

4.13 With regard to SRR9 the Data Protection Manager and Information Governance team ensure that the Council is able to evidence compliance of Article 25 under the general data protection regulations (GDPR) in that:

- Data changes follow a strict procedure that ensures appropriate assessments are undertaken that provide sufficient assurance around data protection, confidentiality and information rights compliance;
- Adequate organisational and technical controls are in place to support the compliant and secure collection, creation, sharing and storage of data;
- Adequate and appropriate guidance, awareness and training to both maintain and improve on our current compliance status;
- Sufficient levels of responsibility are documented throughout our suite of policies, procedures, standards and guidance.

4.14 A more in-depth overview of the controls and mitigating actions in place are covered within the risk register in the appendix to this document. These controls alongside the way in which data protection responsibility is achieved throughout the council results in this risk level being acceptable, given that the potential for any harm or distress could be high in the event of a serious incident where the outcome is due to failing to follow or comply with the above controls.

4.15 The Information Governance team works actively with service areas and through the directorate representatives who make up the Forum for Information Governance and Assurance and aim to improve on these outcomes by sharing the data collected, ensuring lessons learnt is taken from any breach experienced and ensuring the that appropriate action is taken swiftly whenever a high threat or risk is identified such as with emerging technology or in event of any data breaches.

## **5. Financial Information**

5.1 There are no direct financial implications arising from this report, however effective risk management and reporting of risks supports and contributes to the delivery of good financial management.

5.2 In relation to SRR8, There may be a requirement for financial investment for additional cyber security resources and/or tools in the future; these requests will be made via the appropriate route. With regard to SRR9 the financial implications of a significant data breach through noncompliance of the regulations is documented accordingly within the risk register to ensure the council is fully aware of the potential impact. There is also an increased risk of financial loss due to compensation claims where any such serious incident results in severe harm or distress to those data subjects concerned.

## **6. Reducing Inequalities**

6.1 Effective governance arrangements ensure a focus on delivering of Corporate Plan objectives, a key driver of which is reducing inequalities.

## **7. Decide**

7.1 Audit Committee are asked to consider the updates made to the Strategic Risk Register and may wish to comment.

## **8. Respond**

8.1 Audit Committee is required to ensure that it receives reports on risk management on a regular basis and takes appropriate action to ensure that strategic business risks are being actively managed. This report enables Audit Committee to exercise its responsibilities in respect of risk management by reviewing the current SRR; calling in key business risks for review; and seeking assurance that risk management is thoroughly embedded within the organisation.

## **9. Review**

9.1 The Risk Management Strategy sets out the formal review and reporting points for risks throughout the year and these will continue to be followed, with feedback on the actions set out within this report incorporated into those updates.

### **Officer Contact:**

Vicky Buckley, Head of Finance and Assurance, ☎01922 652326,

✉ [vicky.buckley@walsall.gov.uk](mailto:vicky.buckley@walsall.gov.uk)