


REPORT TO AUDIT AND RISK ASSURANCE COMMITTEE

19 October 2017

Subject:	Strategic Risk Register Update
Director:	Executive Director – Resources
Contribution towards Vision 2030:	
Contact Officer(s):	Narinder Phagura Business Partner - Audit, Fraud, Risk and Insurance narinder_phagura@sandwell.gov.uk

DECISION RECOMMENDATIONS

That Audit and Risk Assurance Committee:

1. Review and comment upon the accompanying report.

1 **PURPOSE OF THE REPORT**

1.1 At the last meeting of the Committee, members requested consideration be given to the following matters for inclusion in the SRR:

- Proposals for a wider cyber security strategy in the West Midlands Combined Authority;
- The council's preparedness in the event of an emergency, including a terrorist attack; and

ILO UNCLASSIFIED

- The requirement under the new General Data Protection Regulations

This report sets out the further consideration of each of these matters.

2 IMPLICATIONS FOR SANDWELL'S VISION

- 2.1 Effective risk management is a key element of good corporate governance and is essential to the overall performance of the council in meeting its vision 2030. Good risk management will ensure that resources are used efficiently and effectively in the delivery of the Sandwell vision and that assets and resources are protected against risk in the most efficient way.

3 BACKGROUND AND MAIN CONSIDERATIONS

- 3.1 The council is no different to any organisation, and will always face risks in achieving its vision and objectives. Sound risk management can be seen as the clear identification and management of such risks to an acceptable level.
- 3.2 The strategic risk register does not include all of the risks that the council faces. It represents the most significant risks that could potentially impact on the achievement of the council's corporate priorities and vision. Other risks are captured within directorate, operational, programme, project or partnership risk registers in line with the council's corporate risk management framework and strategy.
- 3.3 Ownership of the individual strategic risks is assigned to directors, who have responsibility to:
- Consider and agree the risk description
 - Assess the current risk score based upon the controls in place and the assurances they have received on the adequacy and effectiveness of these controls
 - Implement mitigating actions to reduce the risk scores where necessary, in order to deliver the required risk score by the target date
 - Keep Cabinet Members informed of the risk and the implementation of mitigating actions.

Further ongoing reviews are then undertaken by the Management Board.

- 3.4 A summary of the strategic risks is included at Appendix A of this report.

ILO UNCLASSIFIED

4 THE CURRENT POSITION

4.1 Since last reported, two new risks have been added to the SRR as follows:

- Risk 47 – Maximising opportunities from the West Midlands Combined Authority (WMCA)
- Risk 48 – Vision 2030

4.2 At the previous meeting of the Committee in August 2017, members requested consideration be given to the following matters for inclusion in the SRR:

- Proposals for a wider cyber security strategy in the West Midlands Combined Authority;
- The council's preparedness in the event of an emergency such as Grenfell and a terrorist attack; and
- The requirement under the new General Data Protection Regulations

This report sets out the consideration of each of these matters.

Cyber security strategy

4.3 The SRR includes at risk 42a, a risk in respect of cyber security. Whilst not a risk in its own right, proposals for a wider cyber security strategy could be considered as a mitigation to this risk.

4.4 As cyber security is a high profile topic, regular meetings of the ICT Heads of Service across the WMCA take place where approaches to cyber security are discussed and ideas and tools are shared.

4.5 Following the Wannacry incident earlier this year, further discussions took place across the WMCA so that there was a good understanding of each organisation's approach to cyber security. The discussions also included the potential for negotiating a WMCA contract which would provide each organisation with third party forensic expertise in the event of one or more of the WMCA authorities experiencing a compromise. Work is being done to consider this further.

- 4.6 Sandwell is further developing its cyber security strategy and this will seek to collaborate and share thoughts and ideas with our WMCA partners through the ICT Managers Group. The ICT Managers Group will continue to discuss closer collaboration and look for shared working opportunities and strategies where appropriate.
- 4.7 Further updates will be provided to the Committee as part of the update on the cyber security strategic risk.

Emergency planning and terrorism

- 4.8 The SRR includes at risk 6a, a risk in respect of the council's emergency planning arrangements. The risk description has been amended to clarify that this risk deals with all emergencies- at a national, regional and local level. As part of the mitigations and emergency response measures in place, this risk also considers the arrangements the council has in place to deal with any type of major emergency, be it arising from severe weather, terrorism, chemical leaks, fire, etc. In these instances, the council has a number of emergency plans in place, including, the Sandwell MBC Emergency Plan; School's Emergency and Business Continuity Plan; Emergency Assistance Centre Plan; a Rest Centre Plan; Sandwell Evacuation Plan and a Temporary Mortuary Plan.
- 4.9 Some of the measures the council will have in place will be to support other emergency services such as the Police in the event of a terrorist incident or the Fire Service in an incident such as Grenfell. In these instances, the council's response is based on consequence management whereby the council will assist in mitigating the impact of such an incident through the triggering and delivery of one or a number of the plans noted above. For example, the evacuation plan will be triggered whether it is major emergency arising from a flood, fire, threat or a bomb alert.
- 4.10 The emergency plans that have been compiled are based upon the risks that have been identified by the Local Resilience Forum and contained within the Community Risk Register. These plans are distributed to relevant Officers, Directors and Partners, as well as made publicly available where appropriate. They are tested on a regular basis via planned single and multi-agency exercises and real events (for example, in recent times the council has experienced the Tipton bomb incident and a tower block fire incident). The plans are reviewed on timescales appropriate to the risk and after each incident or exercise where necessary.

- 4.11 Emergency Planning awareness briefing is also provided as part of the member development/ induction programme where further details can be provided on how the council would deal with various specific scenarios.
- 4.12 As a result of the above, it considered that separate risks for every type of incident is not required for inclusion in the SRR as the current strategic risk effectively captures these events and incidences.

General Data Protection Regulations (GDPR)

- 4.13 Members are requested to note that the SRR includes at risk 21a, the risk in respect of GDPR and the Freedom of Information Act. Progress on the steps being taken by the council to mitigate this risk are included in each risk report. Members are requested to note the below.
- 4.14 The council must be compliant with the GDPR by no later than 25 May 2018. The Information Commissioner's Office will monitor compliance with GDPR as part of its functions. The ICO can impose significant fines should the council fail to comply with the requirements of GDPR.
- 4.15 The Director – Monitoring Officer has put in place an Officer Information Governance Board ('IGB') that is made up of key officers from across council directorates. The officers on the IGB all have specific responsibilities for information governance within their respective directorates. An action plan is being developed and all actions will be delivered through the IGB to ensure effective co-ordination and consistency across the council; this will include engagement with and training for all Elected Members. The performance of the IGB will be managed through the Corporate Governance Group that is made up of senior officers from key services that lead on information governance and related functions across the council, such as, Internal Audit, Risk and Insurance, and Law and Governance. The Corporate Governance Group provides assurance to the Chief Executive's Management Team in relation to the council's governance arrangements and matters.
- 4.16 Periodic updates will be provided to the Audit and Risk Assurance Committee on the implementation of GDPR through the update on the strategic risk register.

5 CONSULTATION (CUSTOMERS AND OTHER STAKEHOLDERS)

- 5.1 The review and update of each strategic risk, has been discussed with the risk owners (as noted at Appendix A) and reported to the Management team.

ILO UNCLASSIFIED

6 ALTERNATIVE OPTIONS

- 6.1 Whilst this report does not require a decision and therefore, alternative options do not need to be considered, when measures are being considered for the mitigation of each of the strategic risks, this does take into account any alternative options available.

7 STRATEGIC RESOURCE IMPLICATIONS

- 7.1 The authority's Corporate Risk Management Strategy (CRMS) requires close identification and alignment of risks to budget planning processes. In this way, the identification and management of its key risks informs the authority's allocation of resources.
- 7.2 The authority's budget planning process incorporates financial and other resources required to manage the authority's risks.

LEGAL AND GOVERNANCE CONSIDERATIONS

- 8.1 The purpose of risk management is to assist in the achievement of the Sandwell vision and the authority's statutory responsibilities.
- 8.2 There are numerous standards applicable to the management of risk within the local authority sector. Included amongst these is guidance from CIPFA/Solace, the British Standards Institute (BSI) and a set of joint standards published by the Institute of Risk Management (IRM), Alarm (The public sector risk management association) and AIRMIC (Association of Risk Managers in Industry and Commerce). Evidence that robust management of the authority's strategic risks is being undertaken demonstrates compliance with these standards.

9 EQUALITY IMPACT ASSESSMENT

- 9.1 As a decision is not being sought in this report, it is not necessary to undertake an Equality Impact Assessment.

10 DATA PROTECTION IMPACT ASSESSMENT

- 10.1 As a decision is not being sought in this report, it is not necessary to undertake a Data Protection Impact Assessment.

11 CRIME AND DISORDER AND RISK ASSESSMENT

ILO UNCLASSIFIED

11.1 There are no crime and disorder risks arising from this report.

12 SUSTAINABILITY OF PROPOSALS

12.1 There are no direct sustainability issues arising from this report.

13 HEALTH AND WELLBEING IMPLICATIONS

13.1 There are no direct health and wellbeing implications from this report.

14 IMPACT ON ANY COUNCIL MANAGED PROPERTY OR LAND

14.1 There is no direct impact on any council managed property or land from this report.

15 CONCLUSIONS AND SUMMARY OF REASONS FOR THE RECOMMENDATIONS

15.1 The purpose of the report is to update the Audit and Risk Assurance Committee with the council's key strategic risks as summarised in Appendix A.

16 BACKGROUND PAPERS

16.1 None.

17 APPENDICES:

Strategic risk register summary.

Darren Carter
Executive Director – Resources and s151 Officer

ILO UNCLASSIFIED