

Report to: Governance and Audit Committee

Date: 1 November 2018

Subject: **Risk Management Update**

Director(s): Angela Taylor, Director, Resources

Author(s): Louise Porter

1 Purpose of this report

- 1.1 To provide an update on corporate risk management issues and a progress update on actions related to data protection.

2 Information

- 2.1 Following endorsement of the Corporate Risk Management Strategy at the July meeting of the Governance and Audit Committee, work has continued on the implementation of measures to further embed risk monitoring and reporting arrangements across the organisation.

Corporate Risk Register

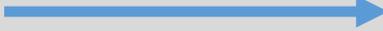
- 2.2 As part of this work each Directorate has undertaken a detailed review of their directorate level risk registers. In light of these updates the corporate risk register for the organisation has also subsequently been updated. A summary of the updated corporate risk register is attached at **Appendix 1**. This includes a summary of the actions being taken to manage each risk and any resulting change in the overall evaluation of them.
- 2.3 As a result of the recent review a number of risks have been escalated to the corporate risk register. This includes one new 'very high' rated risk and six new risks assessed as 'high.'
- 2.4 The additional 'very high' risk relates to the possibility of corporate priorities not being met as a result of outdated organisational infrastructure and processes. While the assessment of this risk has resulted in a 'very high' rating being awarded at present, the projects which have been approved and are now underway as part of the transformation programme and the corporate technology programme are specifically designed to address this risk. The rating of 'very high' is therefore mitigated by the delivery of these critical organisational change programmes that are now moving forward at pace.

2.5 Six additional ‘high’ risks have been added to the corporate risk register. These include items relating to third party suppliers being unable to deliver against contracts, failure to secure sufficient revenue funding to deliver key services and risks associated with changing external conditions which are outside of the control of the Combined Authority.

Risk Appetite Statement

2.6 As a result of the directorate level risk reviews, feedback has also recently been received on the current Risk Appetite Statement resulting in a proposal that the level of financial risk appetite be reduced. This is not related to any specific change in financial circumstances, but instead reflects feedback that the previous assessment of financial risk appetite was on reflection not considered to fully reflect the current position.

2.7 It is therefore proposed to update the Risk Appetite Statement to show the level of financial risk appetite moving from level 3 down to level 2. This would result in the updated Risk Appetite Statement being presented as follows:

Current Risk Appetite:	<i>Low Risk Appetite</i>  <i>High Risk Appetite</i>				
	1	2	3	4	5
Compliance and Regulation					
Operational/Service Delivery					
Financial					
Reputational/Marketing/PR					
Strategic Transformational Change					
Development and Regeneration					
People and Culture					

2.8 The Governance and Audit Committee is requested to provide feedback on this proposed change and also more generally on the current assessment of risk appetite across all categories as presented above.

Regulatory and Compliance Board

2.9 As part of the ongoing internal governance review for the Combined Authority it is proposed to establish a new officer led Regulatory and Compliance Board to provide strategic direction on all regulatory and compliance matters.

2.10 It is intended that this Board will be chaired by the Director, Resources and will cover all areas of regulation including:

- Information governance and data protection;
- Health and safety;
- Internal and external audit; and

- Financial and other key controls
- 2.11 This Board will undertake a vital role in ensuring corporate oversight of all risks relating to regulatory and compliance issues and will be responsible for ensuring that appropriate mitigation measures are in place and that risks are escalated appropriately.
- 2.12 The Regulatory and Compliance Board will also become the formal Board for the escalation of issues relating to data protection/GDPR.

GDPR

- 2.13 The report provided to Governance and Audit Committee on 29 March 2018 gave an update on the work already taken by officers in preparation for GDPR and a subsequent report was provided to the meeting of the Combined Authority on 10 May.
- 2.14 Significant progress has since been made implementing and embedding GDPR throughout the organisation. Key actions taken include:
- The roll out of GDPR e-learning for all staff;
 - Procurement of advanced GDPR training for Information Asset Owners;
 - Approval of a new Data Protection Policy;
 - The provision of 1 minute topic specific guidance documents for staff;
 - The provision of guidance for Members;
 - The creation of a new Information Asset Register and guidance to staff on updating the Register;
 - The drafting of new corporate and project specific privacy notices;
 - The creation of a Data Protection Impact Assessment Procedure and Toolkit;
 - Monitoring and reporting of data breaches via the new Data and Systems Security Incident Policy and Procedure;
 - The variation of all contracts to include GDPR compliant terms and conditions;
 - The destruction of all records beyond retention period previously held in the Halifax record store;
 - The transfer to the West Yorkshire Archives of all records of historical value;
 - The appointment of a Specialist Records Management Officer;
 - The arrangement of a cyber security audit by the Combined Authority's insurers;
 - The creation of an Information Governance Risk Register to feed into the Corporate Risk Register.
- 2.15 The ICT risks identified in the previous report are being addressed initially by way of a free cyber security audit being carried by the Combined Authority's insurers alongside an internal compliance review of the Combined Authority's business applications. Over the coming year the Corporate Technology Programme will address the redesign of network folders, introduce improved data management and information rights management infrastructure, and implement new and refreshed corporate systems. This will address many of

the challenges facing the Combined Authority in the use of current data storage methods.

2.16 The records management risks identified in the previous report are being addressed through the appointment of a specialist Records Management Officer whose role from 7 November will be to implement a records management strategy across the organisation.

2.17 It is also proposed that the Combined Authority's compliance with GDPR will be monitored via a programme of internal audit over the next 7 months.

3 Financial Implications

3.1 There are no financial implications arising from this report.

4 Legal Implications

4.1 There are no legal implications arising from this report.

5 Staffing Implications

5.1 There are no staffing implications arising from this report.

6 External Consultees

6.1 No external consultations have been undertaken.

7 Recommendations

7.1 That members of the Governance and Audit Committee note the update provided in this report and provide feedback on the Corporate Risk Register at **Appendix 1** and the Risk Appetite Statement as presented at 2.7.

8 Background Documents

None.

9 Appendices

Appendix 1 – Corporate Risk Register