


<p>London Borough of Hammersmith & Fulham</p> <p>AUDIT, PENSIONS AND STANDARDS COMMITTEE</p> <p>21 June 2017</p>	
RISK MANAGEMENT	
Report of the Interim Director of Audit, Fraud, Risk, and Insurances	
<p>Part Exempt Report Confidential elements of this report can be found in the exempt agenda.</p>	
<p>Classification: For Information Key Decision: No</p>	
Wards Affected: None	
Accountable Director: Moira Mackie, Interim Director of Audit, Fraud, Risk, and Insurances	
<p>Report Author: Michael Sloniowski, Risk Manager</p>	<p>Contact Details: Tel: 020 8753 2587 E-mail: michael.sloniowski@lbhf.gov.uk</p>

1. EXECUTIVE SUMMARY

1.1. The purpose of this report is to provide the Audit, Pensions, and Standards Committee with:

- a) An oversight of the authority's processes to facilitate the identification and management of its significant business risks.
- b) Oversight of the Corporate and the key Service risks.

1.2. The report enables the Audit, Pensions and Standards Committee fulfil part of its functions as set out in the Committee's terms of reference, to review the Risk Management arrangements of the authority.

2. RECOMMENDATIONS

2.1. The Committee is asked to note the contents of the report;

3. REASONS FOR DECISION

- 3.1. The Chartered Institute of Public Finance and Accountancy's local government risk framework is based on a belief that 'good governance structures enable an authority to pursue its vision effectively as well as underpinning that vision with mechanisms for control and management of risk'. In other words, risk management is implicit in good performance.

4. PROPOSAL AND ISSUES

Directors Assurance Statements

- 4.1. In accordance with regulation 6(1) of the Accounts and Audit (England) Regulations 2015 in relation to the preparation of an Annual Governance Statement, the Council is required to conduct a review at least once a year of the effectiveness of its governance arrangements, including its system of internal control and arrangements for risk management.
- 4.2. To facilitate this, Directors are required to complete and certify a self-assessment questionnaire on at least an annual basis. This questionnaire acknowledges the responsibility of the Director in disseminating corporate messages and monitoring practices that uphold the council's governance framework within their Service.
- 4.3. The self-assessment includes the requirement to comment on the following areas during 2016/17:
- Policy and decision making;
 - Service Planning and Delivery;
 - Strategic and Operational Risk Management;
 - Performance Management;
 - Partnerships with other public bodies, voluntary and community organisations, Arm's Length Management Organisations and Mutuals;
 - Finance and asset management;
 - Staffing;
 - Information governance;
 - The control environment;
 - Programmes and projects;
 - Performance management;
 - Significant control or governance failings reported during the year 2016/17.
- 4.4. Additionally, each Director is required to state whether, in their opinion and considering the Directors self-assessment reports, an appropriate level of control was maintained in their area during the year. All Directors submitted affirmative statements for 2016/17.
- 4.5. There have been two disclosures made in this year's statements, associated with the ongoing issues associated with the Finance and Human Resources Managed Service, legacy casework and data quality associated with a prior

Pensions administrator, the latter mitigated through additional short-term staffing.

4.6. ***The Reporting of Corporate, Organisational Risks***

- 4.7. The approach to managing risk is outlined in the Council's Risk Management Strategy Statement 2017-2020. The Statement encourages innovation and creative approaches to service delivery whilst requiring careful consideration of the risks involved and responding appropriately to manage them.
- 4.8. The Corporate Risk Management Process is aimed at identifying, assessing, prioritising and mitigating the significant risks which could impact on the delivery of the council's objectives (i.e. corporate risks). This process is also aligned with the council's Service Teams Management arrangements. Corporate risks are those concerned with ensuring overall success of Council objectives, and the vitality and viability of the organisation. Materialisation of such risks can have many consequences, for example they could significantly affect the reputation of the Council, present significant financial costs or be affected by significant tests of its resilience as most recently seen in the terrorist attacks at Westminster and Manchester.

Corporate Risks

4.9. ***Resilience – High Risk (Appendix 2, Business Continuity Risks)***

The National Health Service Cyber Security attack – WannaCry.

- 4.10. The WannaCry ransomware attack affected businesses around the world, mostly Asia and Europe were worst hit. On the 12th May the National Health Service IT systems were impacted by a major incident because of a Cyber-attack. The incident, which is described as ransomware, encrypts data, and then prompts for payment to unencrypt. It is likely that such an incident was caused by opening of an attachment containing a zero-day virus from an email received into the NHS. Our service providers protect our network by keeping security patches up to date, and where an infected email is detected by scanning the email system and deleting those.
- 4.11. A zero-day vulnerability refers to a hole in software that is, at the time unknown. Hackers then exploit this security hole before IT and Security providers become aware and can fix it. This exploit is called a zero-day attack. In response a message to all staff was placed on the Council's Intranet page providing advice on handling suspicious e-mail traffic and to remain vigilant whilst the IT service updated protection. Whilst the size of the ransom was small, between \$300 to \$600 the reports of disruption to the operations within the NHS and affected companies while the clean up to affected systems took place was significant.
- 4.12. On the 15th May the Council's Business Continuity and Information Management Teams jointly promoted Business Continuity Awareness Week helping make LBHF a resilient organisation by keeping information and systems secure, providing advice on;

- countering cyber threats;
- the tips published by the Business Continuity Institute on the Business Continuity Awareness Week (15-19 May) posters displayed in the Town Hall;
- the LBHF information security policy and supporting codes of practice;
- completing the mandatory information security and data protection induction online training courses.

- 4.13. A meeting of the Council's Service Resilience Group (SRG), representing all Services, took place on the 16th May to discuss the progress of Business Continuity Planning. The Council has Business Continuity Plans in place, currently being refreshed. These are administered on Word and Excel systems stored in the Council's IT folders. SRG considered if Service Continuity plans should be transferred to an on-line electronic, hosted and more dynamic solution so that they operate if the Council's systems are not available for a significant period. Through technology, plans could be made available to Members and Officers on a variety of devices, smart phones, Notebooks/Laptops, Tablets etc. The Business Continuity Service will review the options available to the Council and make proposals to Officers on the Business Delivery Team.
- 4.14. On the 22nd May the City of Manchester was hit by a terror attack. The venue, Manchester Arena was being used for a concert at the time. Following the Manchester incident the Council's Service Resilience Group, chaired by the Head of Emergency Planning met to assess the local situation. Following the meeting actions were immediately implemented that included the work of the local Prevent Team Members, who have been monitoring the ongoing situation, contacting schools providing advice and re-advertising the Workshops to Raise Awareness of the Prevent scheme. The Group also reviewed security and access arrangements to Council buildings, Council Officers were recommended to review the appropriateness of Business Continuity plans and re-assuring communications issued to staff. The Head of Emergency Services maintains an ongoing review of the Council's response here.
- 4.15. **Information and Digital Continuity – Modified Risk**
General Data Protection Regulations.
- 4.16. The General Data Protection Regulations (GDPR) will apply in the United Kingdom from 25 May 2018. The government has confirmed that the UK's decision to leave the European Union will not affect the commencement of the GDPR. The Information Commissioners Office is committed to assisting businesses and public bodies to prepare to meet the requirements of the GDPR ahead of May 2018 and beyond.

The GDPR applies to 'controllers' and 'processors'. The definitions are broadly the same as under the Data Protection Act – i.e. the controller says how and why personal data is processed and the processor acts on the controller's behalf. The Council is subject to the Data Protection Act, and is subject to the Regulations.

- 4.17. For the Council keeping Human Resources records, customer lists, or contact details etc., the change to the definition should make little practical difference. The Council holds information that falls within the scope of the Data Protection Act, it will also fall within the scope of the GDPR. Under the GDPR, the data protection principles set out the main responsibilities for organisations. The principles are like those in the Data Protection Act, with added detail at certain points and a new accountability requirement. The most significant addition is the accountability principle. The GDPR requires the Council to show how it complies with the principles – for example by documenting the decisions taken about a processing activity.
- 4.18. The Interim Chief Information Officer met with Council Officers on the 24th May 2017 to discuss the risks and solutions. Several actions, outlined below, were agreed and are to be taken forward by a Project Team with a lead sponsoring Officer on the Council's Business Delivery Team.
- Review the data protection policy and make it ready for GDPR, including recommendations of the voluntary Information Commissioner's Office audit.
 - The General Data Protection Regulations will be incorporated into the refresh of the LBHF IT technology.
 - A working group to progress actions will be established.
 - The Council's Legal Services will review and check wording correct for all new contracts.
 - The Project Team will review other work that the Information Governance for London and London Chief Information Officers are doing to ensure consistency and minimise effort.
 - Identify a Senior Responsible Officer for this project.

4.19. ***Partnerships – New Risk***

- 4.20. Ending of Shared Services, Adults Social Care and Children's Services. A report on the change to Service Provision in these areas has been issued separately to the Audit, Pensions and Standards Committee following the notice to terminate the existing Section 113 agreement by Westminster City Council and the Royal Borough of Kensington and Chelsea. The Project known as Moving On will be led by Members of the Strategic Leadership Team.

4.21. ***Managed Services – High Risk***

The following principal (high) risks remain as identified by the Intelligent Client Function;

- Resources, both from BT and Council resources with the requisite knowledge and experience to deliver remaining activity;
- Remaining activity (as referred to above) will not deliver a solution that meets the business needs;
- The emergence of divergent priorities from the Councils;
- BT does not want to take up the option to extend the contract beyond May 2019;

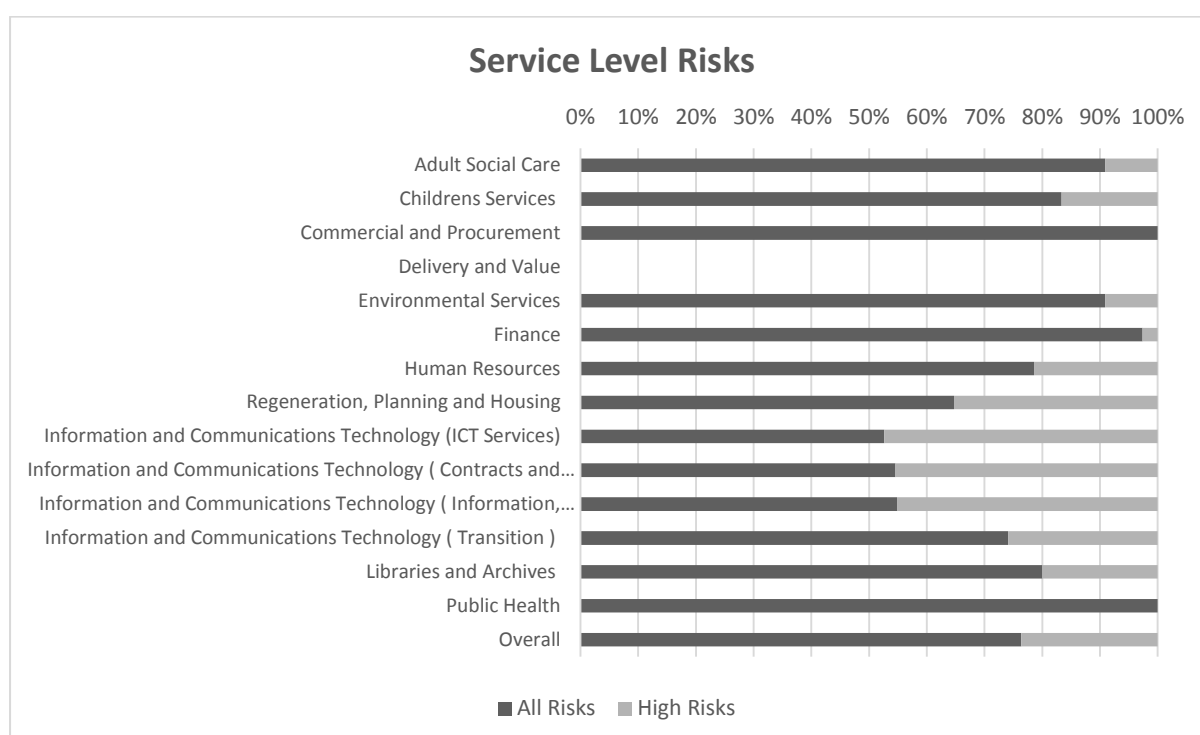
- BT removal of access to programme resources;
- Resolution of commercial discussions.

Other Corporate Risks are unchanged.

4.22. **Service Risks (Appendix 1, Services High Risks Extract Dashboard)**

4.23. At the end of May there were 184 identified active risks on the Council's Service Level risk registers. To ensure risk management process remains effective and aligned to organisational objectives, these are reviewed quarterly by the Service Management teams. The Service Level High Risk Extract Dashboard accompanies this report and is attached as Appendix 1.

Chart 1 Illustrates the percentage of high risks by service.



A process is in place to aid all Services to capture key risks and assess their significance. The methodology adopted by the authority is used to assess and prioritise key risks and to focus attention on those risks that require attention. Significant risks are examined at Service level and any risk that remains significant after existing controls are taken into account (residual risk) are reported quarterly to the Strategic Leadership Team so that they can be considered further.

5. OPTIONS AND ANALYSIS OF OPTIONS

5.1. The report is brought quarterly to provide the Committee with an oversight of the authority's processes to facilitate the identification and management of its significant business risks.

6. CONSULTATION

- 6.1. The Council's risk management process is implemented across Services, Business Units, and Projects. On a quarterly basis each Service Management Team reviews and updates the risks captured on their risk registers and adds any new or emerging risks.
- 6.2. New risks and key changes to current risks are discussed and challenged at Service and Corporate Management Team meetings. Annually each service is encouraged to undertake a full risk review in support of the submission of a Management Assurance Statement.
- 6.3. Key risks are included within relevant Service or Thematic Risk Registers and are also reported to Audit, Pensions, and Standards Committee. This reporting format ensures that the Council's risk management framework remains embedded and the reporting of risks remains "live" across the organisation.

7. EQUALITY IMPLICATIONS

- 7.1. There are no equality or diversity issues arising from this report.

8. LEGAL IMPLICATIONS

- 8.1. The Council has a responsibility for financial management under the Accounts and Audit Regulations (2015) which requires the Council to have a sound system of internal control, which includes arrangements for the management of risk. The Council is also required to conduct a review at least once a year of its systems of internal control. This report and the enclosed documents assist the Council's compliance with this requirement.

9. FINANCIAL IMPLICATIONS

- 9.1. There are no direct financial implications arising from this report.

10. IMPLICATIONS FOR BUSINESS

- 10.1. There are no direct implications for business arising from this report.

11. OTHER IMPLICATION PARAGRAPHS

RISK MANAGEMENT

- 11.1. The expectations of CIPFA/SOLACE and the Financial Reporting Council are that the systems of risk management and internal control should include: risk assessment; management or mitigation of risks, including the use of control processes; information and communication systems; and processes for monitoring and reviewing their continuing effectiveness.
- 11.2. The risk management and internal control systems should also be embedded in the operations of the council and can respond quickly to evolving business

risks, whether they arise from factors within the council or from changes in the business environment. These systems should not be a periodic compliance exercise, but instead as an integral part of the council's day to day business processes.

12. BACKGROUND PAPERS USED IN PREPARING THIS REPORT

None.

LIST OF APPENDICES:

NOTE: The following appendices can be found in the exempt agenda

Appendix 1, Services High Level Risk Extract Dashboard

Appendix 2, Business Continuity High Level Risk Extract Dashboard