AUDIT & STANDARDS COMMITTEE	**Agenda Item 47** Brighton & Hove City Council

Subject:		**Information Management Risk Update (SR10)**		
Date of Meeting:		**18th November 2014**		
Report of:		**Executive Director, Finance and Resources**		
Contact Officer:	**Name:**	**Mark Watson**	**Tel:**	**29-1585**
	Email:	**Mark.watson@brighton-hove.gov.uk**		
Ward(s) affected:		**All**		

FOR GENERAL RELEASE

1. PURPOSE OF REPORT AND POLICY CONTEXT

1.1 The purpose of this report is to update the Audit and Standards Committee on the ongoing work to mitigate the corporate risk SR10, Information Management.

2. RECOMMENDATIONS:

2.1 That the Audit and Standards Committee notes the report.

3. CONTEXT/ BACKGROUND INFORMATION

Introduction

3.1 Strategic Information Management is an essential discipline in the good governance of any organisation and in its mature relationships with partners. This is especially true in an organisation of the scale and complexity of BHCC where information is the life blood of its business. Good information management and information security practice mitigates risk of information loss and enables the full exploitation of the information the organisation holds. This results in better decision making (based on good quality information) to deliver improved citizen and client experiences and efficient service delivery (e.g. sharing information with partner agencies, collecting information once and reusing many times).Effective information management and security also increases public confidence and helps avoid any potentially damaging action being taken against the council by the information Commissioners Office.

Background

3.2 BHCC holds a huge amount of both sensitive and non-sensitive information. The majority of planning records are a good example of non-sensitive information as much of this is available in the public domain. Information about children and families held by Children’s Social Care is at the other end of the sensitive spectrum. This is an example of information that should be afforded the greatest care and should be shared amongst professionals on a need to know basis. Any loss could cause families significant distress and the council reputational damage. This may impact on our partners' willingness to collaborate in service provision. However, this is a complex area as not sharing information appropriately can also place children at risk. A balance must therefore be achieved and education of our staff which gives them the confidence to share appropriately and securely is therefore crucial.

3.3 Good examples of the implementation of robust information governance practices are in Children's Services in the Multi Agency Safeguarding Hub (MASH) and the Early Help Hub. Both these services are based on partnership working and integrated practice where effective information sharing is a crucial element. The same is true in Adult Social Care where closer working with the Health sector and information sharing across agencies will enable these new partnership working arrangements to deliver the efficiencies and service improvements that support the City's outcomes.

Risk and Impact

3.4 The Information Commissioner's Office (ICO) commonly takes action against organisations found to have been negligent in ensuring they are fully compliant with their obligations under Data Protection Act and the Freedom of Information Act. This could include action being taken even when the loss is a consequence of human error, if the ICO judges that staff have been inadequately educated in Information Governance standards and that there is therefore a heightened risk of data loss.

Failure to comply with the Acts could result in:

- Financial penalties of up to £500,000 per breach. The highest fine to date is £325,000. The average fine is approximately £113,000.
- Loss of reputation and public confidence in the council and the services it provides.
- Personal liability for any member of staff who unlawfully obtains information, or for managers who negligently allow employees to unlawfully obtain information.

3.5 Equally important is the requirement from central government, enforced by the Communications and Electronics Security Group (CESG) and Cabinet Office, that we comply with the Public Service Network (PSN) Code of Connection (CoCo) technical security standards. Failure to comply could result in disconnection from the Public Sector Network and consequent inability to deliver critical council services such as Revenues and Benefits and communications with police and health services.

Mitigation

3.6 Over the last 18 months we have been making some urgent improvements to the technical security of our IT network and information systems.

3.7 So far we have completed the migration to a new Operating System (Windows 7) and upgraded to Office 2010, implemented new firewalls, Network scanning software, Protective Monitoring and Protective Marking on GCSx mail, 2 Factor Authentication, encrypted the entire laptop estate and USBs (portable storage/pen drives), provided managed endpoints (council laptops) to mobile secure information users, separated GCSx (secure government exchange) and .gov.uk email accounts and more.

3.8 There have also been challenges over the last 18 months and not all our changes have been positive for users. We are aware for instance that the implementation of GCSx mail has presented some significant limitations for some users. We propose to address this through the provision of an alternative, more user friendly encrypted email tool. This can be deployed to both Members and staff reducing significantly the number of users who will need to use GCSx mail.

3.9 Nonetheless, the work already completed has significantly improved technical security standards and enabled us to comply with stringent government security standards set by the CESG. This is reflected in BHCC having achieved PSN CoCo compliance for both 2013 and 2014. However, there is a residual risk that this will introduce organisational complacency. Technical security is only part of the mitigation; arguably more difficult to address is the culture of the organisation and the behaviour of staff.

3.10 In order to achieve compliance in 2015 we will need to further improve our technical infrastructure as the requirements continue to increase. This is an extremely challenging set of requirements but will nonetheless provide us with a more robust, efficient and modern environment which will be more reliable and stable into the future.

Actions to address cultural and behavioural change;

3.13 The Information Management Board (IMB) has been established at board level as required by the ICO. It is chaired by the Executive Director, Finance and Resources and is advised by the Senior Information Risk Owner, Head of Legal and Democratic Services. Both our Caldicott Guardians, (Executive Director, Children's Services and Executive Director Adult Social Care) are members of the Board, as are other key senior managers at Corporate Management Team (CMT) level. The Board provides the organisational leadership in Information Management good practice to ensure that the value of our core business information is both protected and exploited to its full potential. The IMB also ensures that the organisation acts upon its legal obligations under the Data Protection Act and Freedom of Information Act. It sets the standards for information management, ensures that these standards are embedded within the organisation, and ensures communication of these key messages to the organisation. For example, the Board reviews and agrees multi-agency data sharing agreements and Privacy Impact Assessments and receives regular key performance indicators and breach reports.

3.14 In addition we have;

- Increased the staffing available to manage and investigate information security and governance matters for:
  - the increased reporting of incidents,

  - development and delivery of training and education
  - increased Freedom of Information requests
  - increased Subject Access Requests
  - new technical security monitoring responsibilities under PSN CoCo
  - relationship with the ICO and PSNA/CESG
  - implementation of records management
- Implemented a complete refresh of policies relating to information management and information security and have published them in one place on the WAVE. The policies set out the expectations and behavioural standards of all staff in relation to their use of information, whatever its format (paper or electronic).
- Refreshed and updated the Information Governance training package and made it available to staff via e-learning
- Initiated a council wide information and security communications plan under the strap-line, 'Safe and Secure'
- Provided face to face and e-learning Information Governance training for Members who are data controllers in their own right
- Provided face to face bespoke training to specific groups of staff
- Completed an information audit across the entire organisation. This will form the basis of a records management approach which will enable better access to information, better quality information and ensure that our information is adequately protected and appropriate sharing is encouraged. Information Asset ownership will be established and responsibilities identified.
- Assessed new multi-agency working initiatives (for example MASH and Early Help Hub) under a Privacy Impact Assessment (PIA) process to ensure an appropriate culture, that balances sharing and privacy, is in place. PIA's are reviewed and signed off by the relevant Executive Director and the Information Management Board.

Why does the risk still persist if we are doing all of the above?

3.15 We send thousands of communications every day to our customers and partners. Over the past year there have been 88 data breaches, of which 79% were due to human error (e.g. incorrectly addressed envelopes, emails and/or incorrect attachments sent to the wrong recipient). Every breach is investigated and where appropriate additional training or controls are put in place. Where breaches are considered to be of a more serious nature, they are reported to the Information Commissioner's Office.

3.16 It is inherently difficult to establish and then truly embed real cultural change in any large and diverse organisation. But this is critical if we are to get true engagement with staff who are extremely busy delivering services at the front line. These requirements can feel like an additional, purely administrative burden. However, it is vital that all of our staff, Members and suppliers working on our behalf, recognise that it is incumbent on all public servants to ensure that the information they hold in trust for citizens is kept safe and treated with the utmost respect.

3.17 It is a requirement of the Information Commissioner that all staff in BHCC undertake annually refreshed Information Governance (IG) training and that this is supported by an audit trail. A new e-learning package has been developed and is currently being rolled out to all staff. Teams have also been identified for bespoke, face-to-face training. All staff, including agency staff, must complete the training. There are no exceptions as the council retains liability for data loss by 3rd parties because it remains the data controller for that originating information. The IG training is part of the compulsory induction programme for all new joiners

4. ANALYSIS & CONSIDERATION OF ANY ALTERNATIVE OPTIONS

4.1 Not applicable

5. COMMUNITY ENGAGEMENT & CONSULTATION

5.1 Not applicable

6. CONCLUSION

6.1 The risk of data loss remains significant and will continue to do so until the culture change which will be brought about by improved education and awareness is fully embedded. The report above describes the ongoing programme of work to achieve this change.

7. FINANCIAL & OTHER IMPLICATIONS:

Financial Implications:

7.1 The financial penalties of non-compliance are outlined in paragraph 3.4. If the council were to be fined the costs would need to be reflected in the Targeted Budget Management projected outurn along with any mitigating costs incurred.

7.2 Ongoing additional costs of improving information management governance and complying with government requirements were included in the additional resources allocated to the ICT service that were agreed at Budget council for 2014/15. In addition, the budget setting assumptions for 2015/16 includes further additional investment for information security, information management and infrastructure that will support the delivery of further mitigating actions.

Finance Officer Consulted: James Hengeveld Date: 06/11/14

Legal Implications:

7.3 The measures identified in the report reflect legal requirements and the steps outlined in paragraph 3.17 will help minimise any risk of breaches of the Data Protection Act or the government's requirements under the Code of Communications.

Lawyer Consulted: Abraham Ghebre-Ghiorghis Date: 06/11/2014

Equalities Implications:

7.4 An Equalities Impact Assessment (EIA) will be conducted against any part of the programme which results in a change to user functionality. Service and or customer service impacts will be addressed by relevant services where identified.

Sustainability Implications:

7.4 Many of the initiatives that contribute to the management and mitigation of information risk contribute to the wider corporate commitment to sustainability and the reduction of carbon emissions e.g. improvements to the underlying IT infrastructure and the migration to the new remote data centre.

Any Other Significant Implications:

7.5 The activity set out in this report supports the corporate plan aim to modernise the council through the delivery of effective, safe, secure and modern working arrangements that can be confidently delivered in partnership with other key agencies across the city.

SUPPORTING DOCUMENTATION

Appendices:

1. None

Documents in Members' Rooms

1. None

Background Documents

1. None

Appendix 1

Crime & Disorder Implications:

1.1 None

Risk and Opportunity Management Implications:

1.2 See main body of report.

Public Health Implications:

1.3 None

Corporate / Citywide Implications:

1.4 See Introduction to this report.