Committee:	Date:
Audit and Risk Management Committee	13th May 2014
Subject: Corporate Risk 16: Information Governance	**Public**
Report of: Chamberlain	**For information**

Summary

The City Corporation routinely manages a considerable volume of information across the organisation that can vary in terms of scale, format, content and complexity.

Information can be personal, reputational and commercially sensitive data, available via online and/or hardcopy. The information explosion' over the past few years has increased the volume and nature of data/content itself: from webpages, video, images to social content. In addition the volume of requests for access to information has increased substantially since legislation such as the Data Protection Act and Freedom of Information Act came into force. The significance of access to and disclosure of business and government information has reached new heights in recent years through a series of high profile cases. While the City Corporation has taken a number of steps in recent years to address the information it handles, access to that information and to comply with current legislation the discipline has evolved substantially and more needs to be done to address the issue.

Issues such as these have highlighted the need for the City Corporation to view information as a business asset. There is a need to approach the handling and care of information in a new way if we are to maximise opportunity as well as mitigating risk.

This paper asks to note the following developments since the last report of 2013:

- Explanation of current 'risk' (Amber) associated with information governance at the City Corporation
- 2013 developments: City partnership with IT partner Agilisys, protective marking and risk mitigation activity over the past year

Recommendations

Members are asked to note this report.

Main Report

Background

1. A variety of legislation covers the governance and management of information in public and private organisations. Key legislation such as the Data Protection Act 1988 (DPA) and The Freedom of Information Act 2000 (FOI) are particularly relevant, yet there may be other Acts which now cover, for example, information security in relation to procurement and investments. However the majority of our current effort is focussed on compliance with DPA and FOI.
2. Increasingly, organisations are required to adhere to growing and evolving guidance around information handling and act upon official guidance provided e.g. Protective Marking of Government Information from HMSC. The Information Asset Maturity Model and Assessment Framework are currently being promoted by the Cabinet Office is a bid to encourage organisations to adopt a strategic rather than reactive approach to information governance in response to the opportunities of information sharing. This reflects a growing call for organisations to improve the way information is shared in order to improve service delivery while complying with government legislation. This calls for a redefinition of 'information risk' in organisations
3. The overall risk for CR16 is Amber. While seemingly the biggest risk posed to the City Corporation is a breach of the Data Protection Act that can incur fines of up to £500,000, this is by no means the only risk. Breach of use of the PSN (public sector network) as well as other regulation breaches may result in security blocks to system access impacting service delivery and/or substantial reputational damage.
4. In addition, failure to consider the possibilities to drive service improvement through appropriate information sharing may result in harm to individuals. For example in case studies involving vulnerable citizens within social care/residents/Police systems this is of particular relevance. The within and between department complexities of the nature (commercial, personal) and flow of information need to be understood and monitored with appropriate guidance and best practice provided where appropriate beyond the walls of DPA and FOI.

Current Risk level 'Amber'

5. The overall risk for CR16 is Amber. The current perceived biggest risk posed to the City Corporation is a breach of the Data Protection Act that can incur fines of up to £500,000. This is because other people's personal information is processed continually by staff, Members, and by third parties on our behalf and there is a medium-high opportunity for error. Processing can range from a small action, such as using a personalised email address, to a large action, such as the relocation to new offices of a paper-based filing system, containing sensitive personal information about children or vulnerable people. However processing also occurs throughout the organisation, including Town Clerk's (HR function and Committee Teams both process sensitive personal information) and the IS Division of Chamberlain's who maintain the security for, and have access to, all information held by the CoL.

6. The risk owner for Corporate Risk 16 is the Chamberlain. However, every Department has a responsibility for the information it holds and a shared responsibility for this risk. In November 2002, a report to the Policy and Resources Committee made this clear: “For effective management I it will be necessary for departments to take responsibility for the co-ordinated implementation and management of the FOIA and DPA”.

Data Protection:

7. The Data Protection Act 1998 (DPA) covers all personal information, and applies to the whole of the City Corporation, although the following are legally separately responsible for their own compliance with the Act: the City of London Police; Sir John Cass's Foundation Primary School; Members with regard to their Ward work; and the Electoral Registration Officer. A breach of any areas of risk as defined by the Data Protection (DP) Principles would be a breach of the Act and is subject to enforcement action, including fines of up to £500,000.
8. DPA compliance is monitored and guided centrally by an Information Officer and Assistant Information Officer, working with an Access to Information Network (AIN). This resourcing is shared with the resourcing of compliance with the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIRs).
9. Mitigating actions against risk of DPA breach include the following ongoing measures:
    - Mandatory training for all staff in Data Protection :
        - 208 staff undertook training in 2013, making a total of 568 since the programme was started in September 2011
        - a total of 18 Members attended training in 2013 including newly elected Members
        - DP compliance is on the Induction Checklist for new joiners
    - Regular engagement with staff via quarterly emails and other relevant communications via corporate channels and the Access to Information Network (AIN)
    - Provision of online guidance around information handling available online
    - Governance arrangements,
    - Systematic Checks and auditing every six months via AIN representative
    - IT security measures to ensure relevant areas have automatic protective marking e.g. social care documentation.
    - Guidance re next steps in the event of a breach is provided online
    - A DP auditing process of compliance checks for the CoL was initiated in November 2013. Audited areas since March 2014 have been: Comptroller and City solicitor's, City Surveyor's Department, Department of the Built Environment, Department of Community and Children's Services, Department of Markets and Consumer Protection, Open Spaces

Department,, Remembrancer's Office, the IS Division, and Corporate HR and Occupational Health. Overall compliance with DP is considered high.

- Following the retirement of the Assistant Town Clerk, Peter Nelson, both the Information Officer and the Assistant Information Officer both report to Neil Davies, Head of Corporate Performance and Development.

Breaches/potential breaches since last report and up to 5 March 2014

- 4 breaches, or potential breaches, reported to the Information Officer.
- Of these, 7 were considered not proven, and of these 5 related to lost or stolen Blackberries, an iPhone and an iPad.
- Of the remaining 2 unproven breaches, one related to wrong use of an email address and one to the publishing of a committee report.
- Most proven breaches all involve accidental disclosure of non-sensitive personal information (within the meaning of the DPA).

Of these:

- 3 related to the failure to blind copy ('Bcc') the names / email addresses of third parties in external emails to multiple recipients;
- 3 related to the unintended sharing of information through a failure to spot the presence of the personal information in documents;
- 1 related to sharing information due to human error.
- While none of the breaches was considered to reach the threshold required for it to be reported to the Information Commissioner, the breach relating to the accidental publishing of non-public minutes concerning personal data has highlighted the need for improved communication and internal reporting of breaches within the City Corporation. It has been noted that such incidents should now include immediate communication to include the relevant Chief Officer, SIRO, Comptroller (as monitoring officer) and Chamberlain. An initial recommendation to review this process will be considered by the Information Management Governance Board at their next meeting in May 2014.

IS security measures in partnership with Agilisys

10. In September 2013, The City Corporation entered into partnership with Agilisys, strategic partner for the delivery of IS services. Agilisys are now responsible for managing the City Corporation's IT infrastructure and have provided the City Corporation with a detailed report of the measures taken to ensure data and cyber/system security, avoid data corruption and hacking/, backup to protect against data loss (personal as well as commercial), compliance with relevant standards such as ISO 27001 and other regulation as required with regular guidance refresh. The report is available on request.
11. Comprehensive procedures already exist for the encryption of USB sticks and password protection of mobile devices, such as ipads. If, therefore, devices are

lost or stolen, any information should remain inaccessible. In addition, staff and Members are required to report such losses as soon as possible to the IS Division, which in turn immediately reports them to the service provider, who immediately terminates service provision. Should there be any delays in reporting by staff or Members to IS Division of loss or theft, this will be investigated by the Information Officer or Assistant Information Officer

12. The Public Sector Network (PSN) is a network of networks of public organisations responsible for the delivery of public services at local, regional and national levels. Complex security compliance demands are in place and CoL has undertaken steps to work the Cabinet Office to meet requirements and is now PSN compliant. Any breaches of PSN compliance result in an information security incident management procedure where internal audit are the single point of contact.

13. The IS Division have recently appointed a Technical Support Officer whose role is to scrutinise all current CoL policy and guidance documents to ensure technical security compliance. The Technical Support Officer will work with the relevant Communications Officer and Information Officers in Town Clerk's department to ensure policies are agreed by all relevant parties, up to date and fit for purpose.

Protective Marking

14. Protective Marking, or guidance around the classification of material as set out by HM Government, has recently undergone changes and those changes come into effect from 1 April 2014. An overview of those classifications in terms of 'as and 'to be' is outlined in Appendix 2. A paper highlighting the HM Government recommendations and our response to those changes was agreed by the Information Management Governance Board in 2013 with respect to the nature of the information we currently handle. The Board agreed that the City Corporation was not required to adopt Protective Marking fully as the majority of the information we hold can be classified as 'official' and, in accordance with official guidelines, does not need to be explicitly marked. However, guidance and information have been provided to those areas that may deal with confidential or sensitive information (e.g. Community and Children's Services). Information about the changes to the protective marking system has been communicated to key departments within the City Corporation and external organisations have taken place via the Joint Emergency Planning and Business Continuity Group. However, further communications at a corporate level informing staff generally about the changes and where to go for further information is now published on the intranet with clear links to relevant pages around information governance.

Information Governance in the City Corporation:

Current Issues and recommendations

15. The current overall approach to information governance within the City Corporation is focussed on risk mitigation to comply with the DPA and FOI. Since the introduction of both Acts a great deal of effort has been channelled into

ensuring CoL compliance: including staff awareness, guidance and training as well as the establishment of an Information Governance Management Board (IMGB).

16. The IMGB while providing useful advice and guidance for individuals and departments on information management has suffered from lack of ownership and organisation as a result of recent staff changes within the IS division. However with the recent staff changes in the IS Division, the IMGB will be reinstated and reinvigorated to review and refresh policy and communications where relevant fit for the digital age.

17. New legislation and guidance on the value of information as a business asset is evolving with great speed. The City Corporation risks being on the backfoot if it does not seize the opportunity to explore the opportunities as well as the risks, and focus is only on mitigation of information risk could result in 'compliance paralysis' which can hinder innovative thinking.

18. Information cost: contract arrangements with our IS partners Agilisys mean the City Corporation has reduced the potential costs of data storage considerably. However, there is a cost risk involved in the longer term unless we install lifecycle information management (creation, distribution, use, maintenance, disposal) more fully in the City Corporation. Therefore, development of guidance and communication in this area will be a remit of the IMGB. Model 1 illustrates the connection between opportunity, cost and compliance with relation to information.

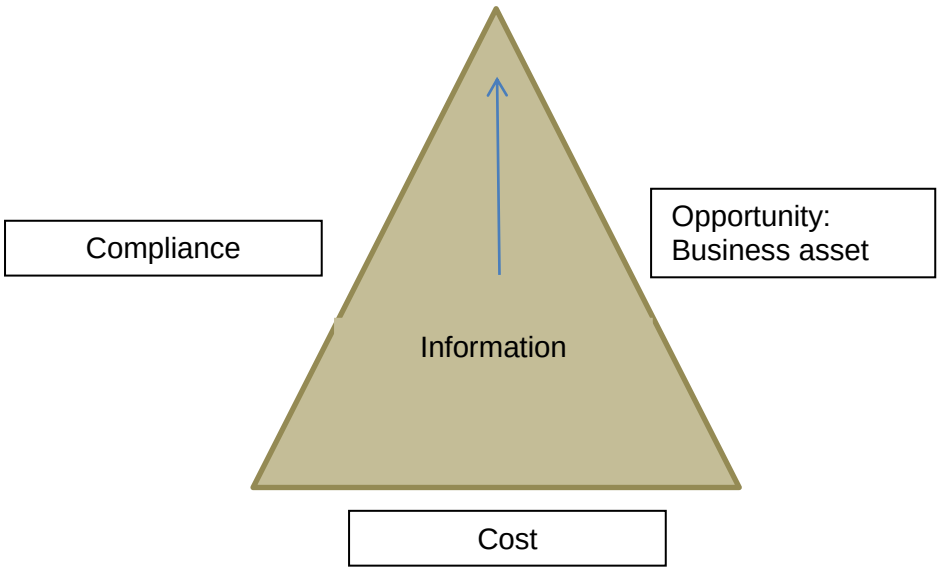
19. Furthermore, other organisations including the City of London Police, other local authorities and public sector organisations are adopting a more 'discipline wide' approach to information strategy beyond mitigation of risk where terms of reference for governance groups include opportunities to share data, resources etc.

Proposed next steps

20. After initial consultation with relevant colleagues within the 'information' and 'knowledge' field in the City Corporation, as well as official best practice the following next steps and timetable is proposed:

Action	Timetable
Reinvigorate and re-instate the IMGB with clear terms of reference, accountability and governance	Spring 2014
Agree relevant policy and guidance revision against the following e.g. information lifecycle, access, sharing and disclosure, use of social media, digital platform and device use in line with wider project and programme delivery organisational strategy and values.	Summer 2014
Work with colleagues in IS and HR to develop appropriate policy and guidance for knowledge capture and sharing within the City Corporation in line with programme of change work	Summer 2014
Board agree appropriate communications and training against policies going forward	Autumn 2014

Model 1



Conclusion

21. A more holistic approach to Information Governance where key experts (policy, IT, training, social media) work together on a fresh programme of activity via the IMGB, covering legislation, policy, education, training, communication and measurement of success is suggested.
22. At present it is unlikely that the net risk could move from Amber to Green, given that personal data processing is such a considerable, widespread and routine activity within most of our functions, and the continuing possibility of human error. However improved communication and awareness of this

Appendices

- **Appendix 1: Risk Supporting Statement: CR16**
- **Appendix 2: Protective Marking Outline**

Graham Bell
Chief Information Officer
T: 0207 332 1307
E: Graham.Bell@cityoflondon.gov.uk

Appendix Two: Protective Marking 'From' and 'To Be' from April 1 2014

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

The new Government Security Classification comes into effect on the 1st April 2014 replacing the Government Protective Marking Scheme (GPMS). In summary, the new policy rationalises the existing six tier protective marking scheme into a three tier model.

At the IMGB in October 2013 it was agreed that this model is not mandatory for CoL.

Further communications and a 'user guide' for key departments such as Community and Children's Services is currently underway as this report is submitted.

Classification	
Government Protective Marking Scheme 'As Is'	Government Security classification policy 'To Be'
Unclassified	Official
Protect	Official (mostly)
Restricted	Official Official sensitive (some)
Confidential	Official sensitive Secret (some)
Secret	Secret
Top Secret	Top Secret