Information Governance Health Check Report
London Borough of Bromley

Adam Lickorish, Senior Strategic Risk Consultant
Martin Clemmit, Strategic Risk Consultant

November 2018

Zurich Municipal

Contents

Introduction & Methodology

Zurich have been commissioned by London Borough of Bromley (LBB) to review the effectiveness of the organisation's information governance arrangements. In order to measure the maturity of this, a Performance Model has been used which breaks down the relevant activities into seven categories that contribute towards effective information governance arrangements within an organisation:

Leadership and Management	*How well do Senior Management understand and respond to Information Risks?*
Strategy and Policy	*How effective are the strategies and policies for managing for managing information risks?*
People and Training	*How well do individuals understand their specific responsibilities and what is the appetite for learning about information risk management within the organisation?*
Technology and Infrastructure	*How securely is information stored and how well is both digital and physical access to information managed?*
Supply Chain	*How well does the organisation understand how much data is shared with suppliers and how well is it managed?*
Incident Management	*How well is the process for identifying, escalating and responding to a data breach understood and embedded?*
Compliance and Audit	*To what extent does the organisation obtain assurance around the effectiveness of its information management processes?*

The model enables an assessment to be made around the extent to which risk management is having a positive effect on the organisation. The five levels of maturity are as follows:

Level 1 - Aware	Level 2 - In Development	Level 3 - Managed	Level 4 - Integrated	Level 5 - Transformational
This level describes organisations where there is recognition of the importance of good IG but although some policy documentation exists, awareness and consistency of approach is generally poor making it highly vulnerable to information breaches	This level describes organisations where there is development of a structured approach to IG but while the risks are better understood these organisations remain vulnerable to information breaches	This level describes organisations where there is a good understanding of information risks and defined policies and procedures. Controls should reduce exposure to information breaches but there are likely to be inconsistencies in how these applied across the organisation	This level describes organisations where IG is embedded and consistently applied across the organisation. Such organisations seek to continually improve their processes and controls to limit their vulnerability to information breaches.	This level describes organisations where IG is a strategic priority and the use of information is leveraged to drive maximum value. Information risks and trends are proactively monitored and mitigated to minimise the vulnerability to information breaches

Executive Summary

Whilst the benefits of digital transformation are clear a recent poll identified that only 30% of the public have confidence in local government to handle their data and information appropriately. It is therefore essential that information governance needs to be considered as key risk within the Council and in particular with regard to change and transformation projects.

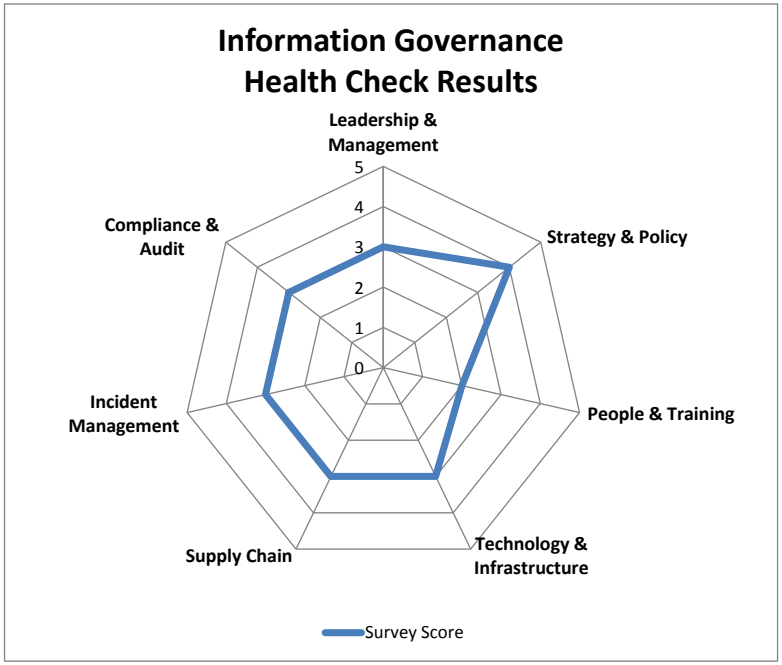
The Information Governance Health Check highlighted an Organisation with strong leadership and policy framework, with the building blocks of a fully effective information governance programme. In all areas the fundamental aspects of an effective information management programme have been established. While the Council scored at 'Level 2 – In Development' in one area, the actions required to improve are relatively easy to attain in the short to medium term.

.

Key areas for improvement identified in the report are:

1. Development of role based training programmes and compliance monitoring and escalation of mandatory training.
2. Risk based action planning to ensure timely close out of information security assessments/audit reports.
3. Further development of performance management metrics to measure effectiveness of the information security programme.
4. Enhance business continuity and disaster recovery arrangements to improve resilience.
5. Improve the management and security of physical records through enforcement of retention periods and clear desk arrangements.

The following pages provide further detail around our conclusions together with recommendations for improvement.



Observations & Recommendations

Leadership & Management

Level 1 Aware	Level 2 In Development	Level 3 Working	Level 4 Integrated	Level 5 Transformational

How well do Senior Management understand and respond to Information Risks?

This section considers:

- Communication and Stakeholder Engagement Strategy
- Clarity of Direction and Strategy
- Senior Level Buy-In and Ownership
- Board Agenda, Strategic Risk Register, Risk Appetite
- Resource Provision

This area is fundamental to setting and maintaining an information risk aware culture across the organisation. It is very difficult for an organisation to make significant progress on the other areas of Information Governance if they are not performing well in this area.

The organisation has all of key roles expected in place, (SIRO, Data Protection Officer, Head of Information Management and Caldicott Guardian). The SIRO and Data Protection Officer roles are held by the Director of Corporate Services and as a result holds a seat on the organisation's leadership team. This also means that control can be deployed directly rather than needing to influence stakeholders on information governance.

The Director of Corporate Services chairs the Information Governance Board that is in place and the membership of the Board includes key individuals and has a focus on sharing experiences, data sharing protocols and training needs.

The organisation had a third party undertake a Data Protection Review in July 2017, from which a significant number of recommendations were made. The organisation has committed to implementing these recommendations and developed an action plan and monitoring process to do this.

Recommendations:

- In light of the recent ransomware attacks that the Organisation has been impacted by, the increasing attack surface and business reliance on IT availability, consideration may wish to be given to including a cyber / data incident risk on the corporate risk register.

- A strong set of cybersecurity metrics should be developed to improve monitoring of the security programme. These could include, for example, (1) Mean time to detect and Mean time to respond, (2) Number of systems with known vulnerabilities, (3) Number of days to deactivate former employee credentials, (4) Percentage of business partners with effective cybersecurity policies, (5) Frequency of review of third party accesses (6) Number of outstanding high-risk findings from security/audit assessments and (7) Completion rates for training programmes.

Observations & Recommendations

Strategy & Policy

Level 1 Aware	Level 2 In Development	Level 3 Working	Level 4 Integrated	Level 5 Transformational

How effective are the strategies and policies for managing information risks?

This section considers:

- Strategy for managing information risks
- Policy for corporate security
- Policy for information risk management

The Information Strategy is currently under review. To be effective, the Strategy should be part of the Business Process Life Cycle and the Council must ensure there is a cooperative dialogue between business areas and information security experts to ensure the Strategy is aligned with Organisational objectives including risk management and corporate governance requirements.

A full range of expected policies are in place which are of good standard with evidence of regular review and update. However, the number of interrelated information policies could lead to confusion when officers are trying to determine which and how the policies relate to their area of responsibility. The approach could be improved by adopting a hierarchal approach to Policy development whereby Tier 1 is considered Organisational Level (e.g. Asset Management), Tier 2 Topic Level (e.g. Records Retention, Information Classification) and Tier 3 Application Level (e.g. Disposal of Records, Access Control).

Information from interviews indicates that the Information Retention and Disposal Process and Guidance is not consistently followed. As well as increasing processing and handling costs the Council is not meeting the Data Protection principle of personal data minimisation. Rationalisation of retention schedules and development of technological solutions to automate record archival and subsequent destruction should be considered.

Recommendations:

- Adopt a hierarchal approach to Information Security Policy development and presentation.

Observations & Recommendations

People & Training

Level 1 Aware	Level 2 In Development	Level 3 Working	Level 4 Integrated	Level 5 Transformational

How well do individuals understand their specific responsibilities and what is the appetite for learning about information risk management within the organisation?

This section considers:

- Culture within the organisation
- Skills and training
- Clarity of roles
- Risk awareness
- Induction for Starters and leavers

This use of information to drive maximum value for stakeholders is a desirable characteristic of organisations today. It is therefore important that employees are aware of their responsibilities and provided with the appropriate training and skills to meet the requirements of achieving this aim.

A key control for managing the human elements of information risk is the e-learning training package. Each of the eight modules is mandatory and should be completed and refreshed annually. The modules are currently being rolled out and the third module – "GDPR" is underway. Whilst training completion is monitored there is no formal follow up/escalation procedure for those that do not. This needs to be addressed to ensure compliance with the training programme.

Recommendations:

- The Information Security Training Programme should include enhanced training for Information Asset Owners as they form a pivotal role in the information asset architecture and management. Line Managers should also receive enhanced training relating to the use and retention of employee records and data.
- Training for Contract Managers should be extended to include matters relating to the oversight of cyber, information and data protection risks in partners and suppliers.
- Information Security Training and Awareness Programmes are most effective at altering behaviours when the employee recognises personal benefit. The Organisation should therefore ensure that training messages highlight how information being provided will help protect employees at home as well as at work.
- Completion of training programmes should be formally monitored and reported on with follow up and escalation to address non-compliance with mandatory requirements.
- Metrics should be defined to assess the effectiveness of awareness training. This could include (1) number of reports of attempted email scams/phishing attempts and (2) number of queries from staff on implementing secure procedures.

Observations & Recommendations

Technology & Infrastructure

Level 1 Aware	Level 2 In Development	Level 3 Working	Level 4 Integrated	Level 5 Transformational

How securely is information stored and how well is both digital and physical access to information managed?

This section considers:

- Computer hardware management
- Secure disposal of IT equipment
- System and Physical site access controls
- Memory and data storage devices
- Email and Document classification / encryption
- Data storage, retention and disposal protocols

The management of day to day operations of the Council's technology and infrastructure is outsourced to BT. The Partner provides system security in a number of key areas including: risk based patch management; intrusion detection logging, password management for all users including system administrators; blocking of malicious and unsuitable internet sites and anti-virus on email exchange and servers. The principle of least privilege is adopted and access to key network infrastructure is suitably controlled. Data on laptops is protected through encryption and portable storage devices (USB) are also protected. USB ports on devices are not locked down, currently allowing both read and write access.

The position regarding the protection of data in transit was a little less clear when discussed with end-users. Egress, an email and file encryption software solution, is available however interviewees gave differing accounts of how and when this is utilised. The matter requires further investigation to determine whether this is a training or implementation issue.

IT and Application Assets are captured on an Asset Register. However the process of updating the Register in terms of new and disposed of assets is not fully effective. The Organisation does recognise these shortcomings and is looking to improve the position.

The storage, retention and disposal of physical records could also be improved. Whilst interviewees were generally aware of published retention schedules and document classifications there was limited confidence that the guidance was being consistently applied. The main concerns are: inappropriate classification of documents; documents retained beyond required retention periods and insecure storage of documents in the context of a clear desk policy.

Printing is controlled in major office locations through the use of pin coded multi-function devices. For other locations, interviewees indicated that printers would be housed in secure or non-public areas. These arrangements are acceptable although further emphasis could be placed on challenging the need to print documents in the first instance.

Observations & Recommendations

Technology & Infrastructure (continued)

Level 1 Aware	Level 2 In Development	Level 3 Working	Level 4 Integrated	Level 5 Transformational

How securely is information stored and how well is both digital and physical access to information managed?

Recommendations:

- Procedures to ensure the IT Asset Register remains accurate and up to date should continue to be developed and reinforced and a process of compliance monitoring introduced.
- Guidelines and requirements for the use of email encryption (Egress) should be reinforced with end-users supported by additional training where required. The implementation of Egress should be reviewed to ensure functionality such as automatic encryption based upon keywords has been considered.
- The Organisation should develop and implement a USB security management system.
- Raise awareness of document classification requirements (as part of the ongoing IG Awareness Programme) to improve compliance with Policy.
- Review and rationalise retention schedules, aiming to reducing the number of retention periods to improve system usability.
- Raise awareness of the Clear Desk Policy and improve compliance through line management monitoring.

Observations & Recommendations

Supply Chain

Level 1 Aware	Level 2 In Development	Level 3 Working	Level 4 Integrated	Level 5 Transformational

How well does the organisation understand how much data is shared with suppliers and how well is it managed?

This section considers:

- Sharing data and requests for information including Freedom of Information and Data Subject Access Requests
- Contract management and supplier performance
- Tendering and procurement processes

The organisation has a dedicated consultant locum lawyer who joined in August 2017. A large amount of activity has been undertaken to address non-compliance in existing contract with new contracts drafted and issued to existing and new suppliers. A small number of suppliers have disputed the change wordings and these are being remediated by Legal Teams. There are 40 outstanding queries that are anticipated to be concluded by end December 2018. Progress and sign off needs to be monitored.

Whilst contracts have been updated to reflect changed requirements of revised Data Protection legislation there does not appear to be a process to ensure these have been returned or followed up where required. Arrangements need to be put in place to ensure timely return of contracts together with Organisational oversight of the position.

The Council needs to further develop procedures, guidance and awareness to ensure Contract Managers and Commissioners are obtaining sufficient assurance that third parties are meeting their information governance and business continuity contractual obligations.

Structures and processes are in place to respond to Data Subject Access Requests (DSARs). However some areas of weakness were have been identified - absence of training on redaction, no sign off requirement for completed DSARs and awareness of protocols for responding to requests from Law Enforcement agencies.

Recommendations:

- On completion of the 40 outstanding queries from contractors, a review should be undertaken to ascertain the response rate and ensure that all of those signed are held on file.
- Redaction training to be provided to staff handling Data Subject Access Requests.
- Procedures need to be refined to ensure a risk based approach to supervisory sign off of Data Subject Access Requests.
- Awareness of protocols for responding to DSARs received from Law Enforcement Agencies needs to be improved.

Observations & Recommendations

Incident Management

Level 1 Aware	Level 2 In Development	Level 3 Working	Level 4 Integrated	Level 5 Transformational

How well is the process for identifying, escalating and responding to a data breach understood and embedded?

This section considers:

- Reporting process
- Definition of incident / breach
- History of breaches
- Business Continuity and Recovery

The Information Security Incident Management Policy (as referenced in the Corporate Information Security Policy) articulates the process for reporting and investigating a breach. This includes the roles and responsibilities of individuals and steps that should be taken as a result. One particular area that was highlighted through the interviews is the lack of awareness of protocols for "out of hours" reporting and thus the potential to not meet the requirement to notify the Information Commissioners Officer of a personal data breach within 72 hours. Out of Hours breach reporting should be covered in Staff Awareness training

Where breaches do occur it is vital that an appropriate and proportionate investigation is undertaken and the lessons are shared and new working practices are established. Through the interview process it was evidenced that breaches are reported well and that key learning is reported at the Information Governance Board.

There are currently no disaster recovery arrangements in place (hot/cold site, mobile site, mirrored site etc) although an off-site backup regime is in place. This introduces a significant weaknesses in Organisational resilience although it is noted that there are plans to address this, subject to funding sign off. Business Continuity Plans have been developed although at Service/Department level they do not consistently respond to disruptive incidents involving the loss of IT. It is important the Business Continuity methodology encourages Service areas to identify critical systems, applications and data which can be used to inform disaster recovery planning and also to consider whether alternative arrangements, such as manual workarounds, need to be implemented.

Two ransomware attacks have occurred over the last 18 months, both fully recovered from. However both were instigated through user error, where a users clicked on a link they shouldn't have.

Recommendations:

- Implement and publicise procedures to ensure prompt internal reporting of data breaches when these occur "out of office hours".
- Ensure that disaster recovery arrangements are properly aligned and strengthened to support business needs and risk management requirements.
- Ensure Business Continuity Management processes identify infrastructure, applications and data required to deliver critical Services and that those critical Service develop contingency arrangements to respond to a loss of IT.

Observations & Recommendations

Compliance & Audit

Level 1 Aware	Level 2 In Development	Level 3 Working	Level 4 Integrated	Level 5 Transformational

To what extent does the organisation obtain assurance around the effectiveness of its information management processes?

This section considers:

- Compliance standards
- Management Monitoring
- Internal Audit
- Undertaking improvement actions

Effective compliance and audit can strongly support a culture of continuous improvement and provide assurance on the effectiveness of the information risk controls.

As previously mentioned, the organisation was subject to a Data Protection Review in July 2017. The action planning that followed this review was subject to an internal audit in October / November 2018. The outcomes of this were that 18 recommendations of 51 that were initially identified are 100% compliant / fully implemented. A further 18 are awaiting further information. Partially implemented actions were also being reviewed.

Built into the 2019 Internal Audit plan is a cyber security gap analysis review against the guidance issued by the Cyber Security Centre. This will cover the configuring of devices and assigning user privileges amongst other elements. The Internal Audit Plan adopts a risk based approach to its programme and Information Governance will remain for the foreseeable period.

Contract management effectiveness on GDPR and information governance will also be included on 2019's plan. Part of this audit will be to ascertain how effectively contract managers are assuring themselves that their suppliers / providers are adhering to their contractual requirements.

Recommendations:

- Establish a programme of office walkthroughs to ensure that staff are following the Council's Clear Desk Policy and locking computer screens when leaving them unattended.
- A risk based action plan to address the outstanding actions from the 2017 Data Protection/GDPR Readiness Review should be implemented and progress reported to the Information Governance Board.
- Guidance should be developed to support Contract Managers in a risk based approach to ensuring compliance with Information Security and Data Protection requirements with Partners and Suppliers.

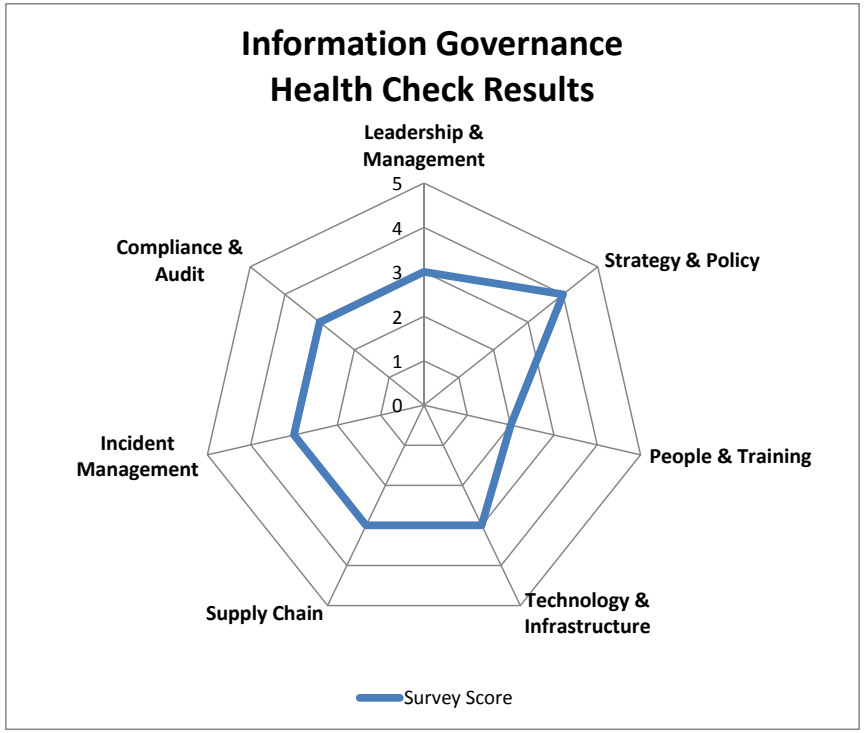
Strengths & Development Areas

Key Strength(s):

- ✓ Sound policies and procedures in place
- ✓ Clear roles and responsibilities
- ✓ Good level of understanding and awareness
- ✓ Framework and supporting documentation
- ✓ A considered risk based approach to Internal Audit
- ✓ Action planning and reporting on completion progress

Areas to focus development:

- Disaster recovery and contingency arrangements
- Training, Education and Awareness
- Embedding the process for the disposal of information assets



Appendix 1 – List of Interviewees

Name	Role
Clive Sheldon	Information Lawyer
David Hogan	Head of Audit
Barrie Cull	Principal Auditor
Mark Bowen	Director of Corporate Services
Vinit Shukle	Head of IT / Senior Information Officer
Charles Obazuaye	Director of HR
Lucinda Bowen	Information Management
Denise Sullivan	Head of HR Business Services
Angela Huggett	Head of HR Strategy & Education
Mark Smeed	Strategic Business Support
Angus Culverwell	Assistant Director, Traffic and Parking
Amit Malik	Head of Deprivation of Liberty Service
Debi Christie / Jenny Macdonald	SEND / Education Welfare
Vicky West / Penny Davies	Head of Adoption and Fostering / Head of Quality Assurance

Appendix 2 – Summary of Recommendations

Section	Recommendation
Leadership and Management	1. In light of the recent ransomware attacks that the Organisation has been impacted by, the increasing attack surface and business reliance on IT availability, consideration may wish to be given to including a cyber / data incident risk on the corporate risk register. 2. A strong set of cybersecurity metrics should be developed to improve monitoring of the security programme.
Strategy and Policy	3. Adopt a hierarchal approach to Information Security Policy development and presentation.
People and Training	4. The Information Security Training Programme should include enhanced training for Information Asset Owners as they form a pivotal role in the information asset architecture and management. Line Managers should also receive enhanced training relating to the use and retention of employee records and data. 5. Training for Contract Managers should be extended to include matters relating to the oversight of cyber, information and data protection risks in partners and suppliers. 6. Information Security Training and Awareness Programmes are most effective at altering behaviours when the employee recognises personal benefit. The Organisation should therefore ensure that training messages highlight how information being provided will help protect employees at home as well as at work. 7. Completion of training programmes should be formally monitored and reported on with follow up and escalation to address non-compliance with mandatory requirements. 8. Metrics should be defined to assess the effectiveness of awareness training. This could include (1) number of reports of attempted email scams/phishing attempts and (2) number of queries from staff on implementing secure procedures.
Technology and Infrastructure	9. Procedures to ensure the IT Asset Register remains accurate and up to date should continue to be developed and reinforced and a process of compliance monitoring introduced. 10. Guidelines and requirements for the use of email encryption (Egress) should be reinforced with end-users supported by additional training where required. The implementation of Egress should be reviewed to ensure functionality such as automatic encryption based upon keywords has been considered. 11. The Organisation should develop and implement a USB security management system. 12. Raise awareness of document classification requirements (as part of the ongoing IG Awareness Programme) to improve compliance with Policy. 13. Review and rationalise retention schedules, aiming to reducing the number of retention periods to improve system usability. 14. Raise awareness of the Clear Desk Policy and improve compliance through line management monitoring.

Appendix 2 – Summary of Recommendations

Section	Recommendation
Supply Chain	15. On completion of the 40 outstanding queries from contractors, a review should be undertaken to ascertain the response rate and ensure that all of those signed are held on file. 16. Redaction training to be provided to staff handling Data Subject Access Requests. 17. Procedures need to be refined to ensure a risk based approach to supervisory sign off of Data Subject Access Requests. 18. Awareness of protocols for responding to DSARs received from Law Enforcement Agencies needs to be improved.
Incident Management	19. Implement and publicise procedures to ensure prompt internal reporting of data breaches when these occur "out of office hours". 20. Ensure that disaster recovery arrangements are properly aligned and strengthened to support business needs and risk management requirements. 21. Ensure Business Continuity Management processes identify infrastructure, applications and data required to deliver critical Services and that those critical Service develop contingency arrangements to respond to a loss of IT.
Compliance and Audit	22. Establish a programme of office walkthroughs to ensure that staff are following the Council's Clear Desk Policy and locking computer screens when leaving them unattended. 23. A risk based action plan to address the outstanding actions from the 2017 Data Protection/GDPR Readiness Review should be implemented and progress reported to the Information Governance Board. 24. Guidance should be developed to support Contract Managers in a risk based approach to ensuring compliance with Information Security and Data Protection requirements with Partners and Suppliers.