SENIOR INFORMATION RISK OWNER

ASSURANCE REPORT

SEPTEMBER 2020

1. INTRODUCTION

This report has been prepared by the Senior Information Risk Owner ("SIRO"). At Bristol City Council the responsibilities of the SIRO are discharged by the Director of Legal and Democratic Services. This report is being presented to the Audit Committee to provide assurance about the policies and procedures that the Council has in place to manage information risk.

In particular, the report provides a summary of the roles and responsibilities within the Council for the management of Information Risk and summarises the key risks that the organisation faces. The report goes on to highlight the key actions that have been delivered over the previous 12-18 months and identifies the planned actions for the next 12 months. It concludes by summarising how the SIRO obtains assurance from the work of the Council to manage Information Risk.

2. ROLES AND RESPONSIBILITIES

Within the Council the responsibility for good Information Risk management sits with all staff at all levels. However, there are certain individuals who have specific responsibilities, which can be summarised as follows.

Senior Information Risk Owner – the SIRO is the senior officer with overall responsibility for Information Risk and has responsibility for sponsoring and promoting Information Governance policy within the Council.

Caldicott Guardian – the Caldicott Guardian is a senior person within a health or social care organisation who makes sure that the personal information about those who use its services is used legally, ethically and appropriately, and that confidentiality is maintained. Caldicott Guardians should be able to provide leadership and informed guidance on complex matters involving confidentiality and information sharing[1].

Head of Information Assurance/Statutory Data Protection Officer – the Head of Information Assurance leads the Information Governance team, and also discharges the role of the Statutory Data Protection Officer. This role is the nominated contacted with the Information Commissioners Office. The Head of Information Assurance is charged with leading and direction the Information Governance activities across the Council and reporting as required to the SIRO.

Information Governance Board (IGB) – the IGB is responsible for ensuring oversight of Information Risk within the Council. It is chaired by the SIRO. Other members of the Board are the Director of Adult Social Care (the Caldicott Guardian) and the Director of Digital Transformation. The Board also has representation from G&R Directorate, Internal Audit and the Statutory Data Protection Officer/Head of Information Assurance.

Information Governance Service – this service is responsible for the development and promotion of Information Governance policies within the Council. The service provides advice and assistance to Information Asset Owners, Lead Custodians and Data Custodians to ensure that local procedures are in place to underpin and implement Information Governance policy within each service area; it leads

---

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/581213/cgmanual.pdf

on BCC's Information Governance control and risk mitigation, supporting service areas to address the risks pertaining to their own services; it manages data security incidents, ensure any incidents are logged, investigated and recommendations implemented; and manages the Council's external relationships with the Information Commissioners Office, National Archives, Cabinet Office, CESG, Local Government Ombudsman.

Information Asset Owners – IAOs are BCC's Directors and are accountable for the information being created, received or obtained by their directorate. They are responsible for ensuring that BCC policies are implemented in the service areas for which they are responsible; for ensuring that their staff are aware of the Information Governance policies that affect them and that they attend or complete training as required; and for fostering a culture of personal responsibility and commitment related to Information Governance matters in their department. This is a key area for further development as noted in section 5 of this report.

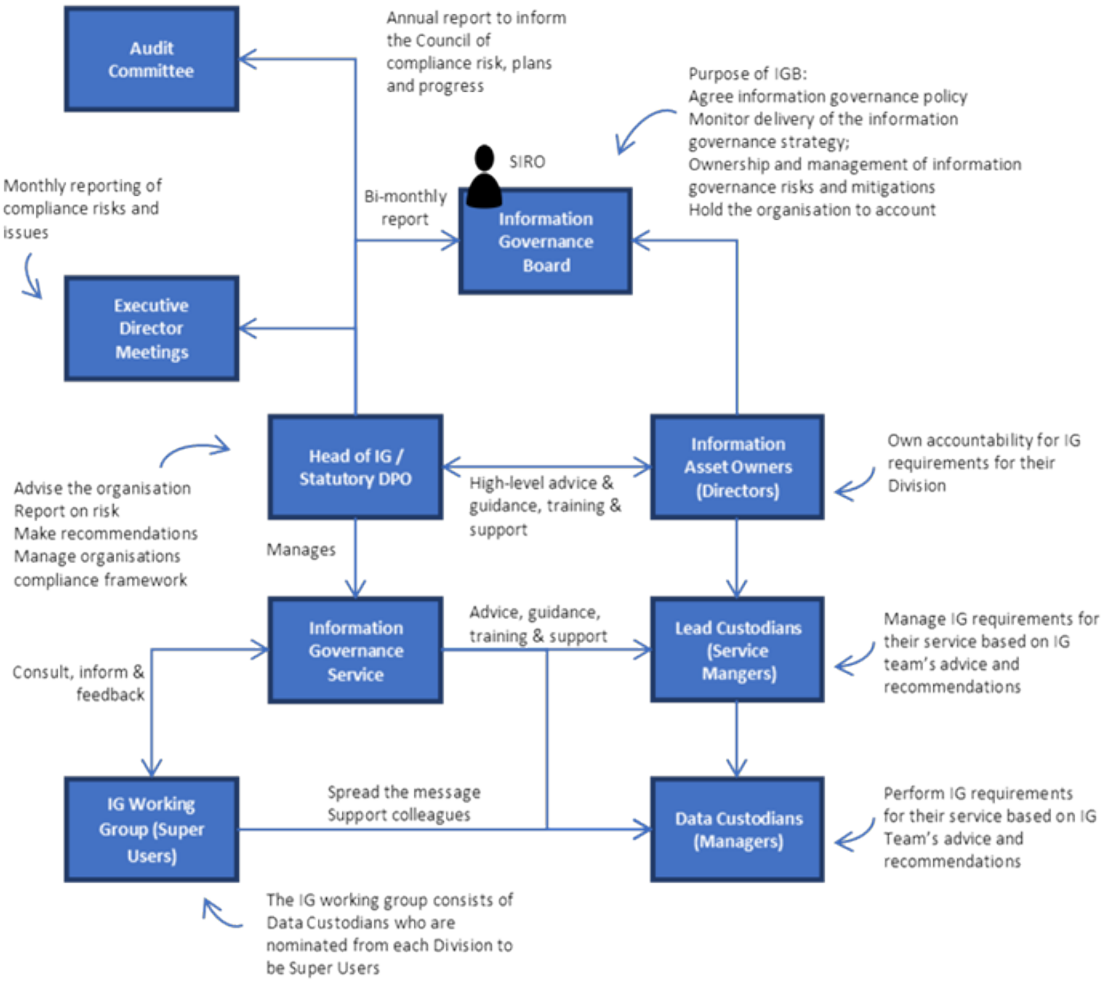
Lead Custodians – Lead Custodians are BCC's Service Managers and they have responsibility for managing the information being created, received or obtained by their service areas. Their responsibilities are similar to Information Asset Owners within their own service areas.

Data Custodians – Data Custodians are tier 4/5 managers and who have day to day responsibility for the information being created, received or obtained by their service area. There may be one or more Data Custodians in each service area, depending on how the service area is organised.

Super Users – Super Users are Data Custodians and represent and are a point of contact with the other Data Custodians within their directorate. There is one or more Super User(s) from each directorate who attend a regular Information Governance Working Group to share learning and develop a consistent approach to Information Governance within the Council.

All staff – All BCC staff, including temporary and agency workers, have a personal responsibility to handle information in accordance with information governance policy, attend security induction training and continue to attend or complete training as required; and report data security incidents and malpractice.

The diagram below shows how the different responsibilities link together to provide a co-ordinated and robust approach to information risk management.



3. INFORMATION RISK

The management of Information Risk is carried out in accordance with the Council's Risk Management Framework.

At an operational level the Information Governance Service is responsible for collating and advising on Information Risk management. All identified operational risks are overseen by the Information Governance Team who provide support to the Information Asset Owners in terms of mitigating activities. A key strand of work is the implementation of an Information Security Management System (ISMS) – this is a series of policies and procedures designed to align with ISO 27001 for the effective and robust management of Information Risk. As part of the work to put in place an ISMS, significant work has been undertaken to collate Information Risks within the Council (encompassing Information Security risks as well as Data Protection risks).

Operational risks will be escalated as appropriate to Directorate Risk Registers which will in turn escalate risks to the Corporate Risk Register. The Council has identified a number of information

risks which are managed through the Council's Corporate Risk Register. An extract of the information risks in the Corporate Risk Register is set out in Appendix A of this report. Full details of the Corporate Risk Register entries relating to information risk, including risk scoring and mitigations are reported separately to the Audit Committee.

4. KEY DELIVERABLES

The following key deliverables have been achieved.

- Creation of Information Governance Service – an Information Governance (IG) Service was established from 1 January 2019 bringing together professional expertise in Data Protection, Freedom of Information (FoI), Information Management and Information Security into one team.
- Information Governance Board – the IGB was established in April 2019. It is chaired by the SIRO, with cross-Council representation, including the Caldicott Guardian, Director of Digital Transformation and Statutory Data Protection Officer/Head of Information Assurance. Internal Audit are also represented on this Board to provide critical challenge and assurance.
- Appointment of Head of Information Assurance – a permanent Head of Information Assurance was appointed in September 2019 to lead on the Information Management, Data Protection and Information Security agenda. This role discharges the functions of the Statutory Data Protection Officer for the Council.
- Information Security Management System – in November 2019 the Council started the work to implement an Information Security Management System which is compliant with ISO27001 certification.
- IT Transformation Programme – the IG Service is embedded in the ITTP programme to ensure that good information governance is embedded in the IT transformation work. The ITTP has also implemented a range of technical controls which provides assurance from an IG perspective (document retention, document classification, Windows 10 and Mobile device security).
- External Certification – the Council has acquired the required assurance certifications, such as PSN and NHS Toolkit.
- Training – mandatory Information Security training and Data Protection training for all BCC staff has been carried out as part of the induction process. Annual refreshers are also undertaken.

5. LOOKING AHEAD

Over the course of the next 12 months the following activities will be progressed to strengthen the Council's approach to information risk management.

- The Council will continue to progress the ISMS implementation.
- Through the Information Governance Team operational risk remediation will be identified and Data Custodians supported to progress risk mitigation plans.
- A General Data Protection Regulation Phase II project will be initiated which will focus on enhancing the Council's policies and procedures relating to data protection to reflect best practice. This will also focus on the need for improved compliance in a number of related

areas including completion of privacy impact assessments, data sharing agreements, records of processing activity, strengthening the role of information asset owners and information retention policies.

- The Council will continue to seek external certification, i.e. PSN, NHS Toolkit.
- An Information Management Strategy will be developed (encompassing, input from information governance, ICT, Insight & Performance and Open Data).
- The information governance agenda will continue to be supported by an Internal Audit Programme of assurance work.
- Executive level training will be provided to the corporate leadership team.
- A Business Continuity exercise relating to Cyber Security incident will be carried out.

6. SIRO ASSURANCE

The purpose of this report is to provide the Audit Committee with assurance that the Council has in place the appropriate policies and procedures to demonstrate good Information Governance. The following activity and actions provide the SIRO with assurance in respect of the management of Information Risk within Bristol City Council.

- Work of Information Governance Board – embedded assurance and senior management oversight.
- Work of Information Governance Team, including escalation of risks to SIRO.
- Statutory Data Protection Officer assurance (monthly reporting to EDMs, SIRO exception reporting or escalation, training, risk registers, ICO management/reporting procedures).
- Data and Information Security Breach reports – monthly reports to EDMs (including details of ICO cases) as well as feedback from the ICO in respect of individual cases.
- Cyber Security compliance and certification – PSN, NHS Toolkit, Police National Database.
- Technical cyber controls – Proofpoint email filtering/spam/phishing and malware detection, Microsoft technical controls (such as Azure Active Directory Identity Protection and Office 365 Advanced Threat Protection amongst others), Bitlocker hard-drive encryption.
- Internal Audit Programme of Work focussed on information governance and data protection – (give examples).
- Managed Phishing exercises with follow up awareness.
- Data Protection and Information Security mandatory training.

7. CONCLUSIONS

The matters raised in this report should provide the Audit Committee with the assurance that the Council's SIRO understands the information risks that it faces and that the Council has in place and/or is developing processes and procedures to effectively manage Information Risk. A number of key deliverables have been put in place over the last 18 months to put the Council on a strong foundation to effectively manage Information Risk. The work planned for the coming 12 months

should provide the Audit Committee with additional assurance that there are appropriate plans in place to ensure that systems and processes are fully embedded at all levels within the Council.

Appendix A: - Corporate Risk Register extract

Ref	Directorate	Service Section	Risk	Threat Risk Description	Key Potential Causes	Key Consequence
L&D 1	Legal & Democratic Services	Information Security	**General Data Protection Regulation (GDPR) compliance.**	If the Council fails to maintain a defensible and compliant response to the Data Protection Act 2018 and General Data Protection Regulation (GDPR) then it will fail to fully comply with its statutory requirements. .	Key potential causes are: • Failure to invest in the required systems, equipment and posts required to implement these regulations. • Failure to adequately train staff in the requirements of the regulations. • Lack of resource (capacity or expertise) to manage Subject Access Requests. • (This risk replaces CRR14 Introduction of the General Data Protection Regulation)	a. Information security incidents resulting in loss of personal data or breach of privacy / confidentiality. b. Safeguarding data breach impacting on safety of vulnerable child or adult. c. Risk of breaching the regulations, and being subject to penalties/fines - Regulations Fines increasing from up to £500,000 to 10-20m Euros of 4% of global turnover, enforced by the Information Commissioners Office on behalf of the European Union. d. Increased litigation. e. Reputational damage.

L&D 2	Legal & Democratic Services	Information Security	**Information Security Management System.**	There is a risk that if the council does not have an Information Security Management System then it will not be able to effectively manage Information Security risks.	Key potential causes are: • Ineffective Information Security Management System, inadequate resources to create and maintain an ISMS, management buy in and support to operate an ISMS	a. Information security incidents resulting in loss of personal data or breach of privacy / confidentiality. b. Safeguarding data breach impacting on safety of vulnerable child or adult. c. Risk of breaching the regulations, and being subject to penalties/fines - Regulations Fines increasing from up to £500,000 to 10-20m Euros of 4% of global turnover, enforced by the Information Commissioners Office on behalf of the European Union. d. Increased litigation. e. Reputational damage.

L&D 3	Legal & Democratic Services	Information Security	**Cyber Security.**	The Council's risk level in regards to Cyber-security is higher than should be expected.	Key potential causes are: • Lack of investment in appropriate technologies. • Reliance on in-house expertise, and self-assessments (PSN). • Lack of formal approach to risk management (ISO27001). • Historic lack of focus.	a. Information security incidents resulting in loss of personal data or breach of privacy / confidentiality. b. Safeguarding data breach impacting on safety of vulnerable child or adult. c. Risk of breaching the regulations, and being subject to penalties/fines - Regulations Fines increasing from up to £500,000 to 10-20m Euros of 4% of global turnover, enforced by the Information Commissioners Office on behalf of the European Union. d. Increased litigation. e. Reputational damage.