SENIOR INFORMATION RISK OWNER

ASSURANCE REPORT

SEPTEMBER 2021

1. INTRODUCTION

At Bristol City Council the responsibility for good Information Risk management sits with all staff at all levels and the management of Information Risk is carried out in accordance with the Council's Risk Management Framework. The effective management of Information Risk is a key function of any large organisation and the Council's approach to Information Risk management has developed over the last few years. This development began with the creation of an Information Governance Service in January 2019, which brought together professional expertise in Data Protection, Freedom of Information (FoI), Information Management and Information Security into one team. In April 2019, an Information Governance Board was established with cross-Council representation, and a permanent Head of Information Assurance was appointed in September 2019 to lead on the Information Management, Data Protection and Information Security agendas.

Work has continued over the last two years to develop a more robust approach to Information Risk management. This report provides an overview of the key aspects of this work. 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 months and identifies the planned actions for the next 12 months. It concludes by summarising how the Senior Information Risk Owner ("SIRO") obtains assurance from the work of the Council to manage Information Risk.

This report has been prepared by the 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.

2. ROLES AND RESPONSIBILITIES

Whilst all staff at Bristol City Council are responsible for information risk management within their own service areas and teams, there are certain individuals who have specific responsibilities in respect of information risk management, 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.

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 Commissioner's 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 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.

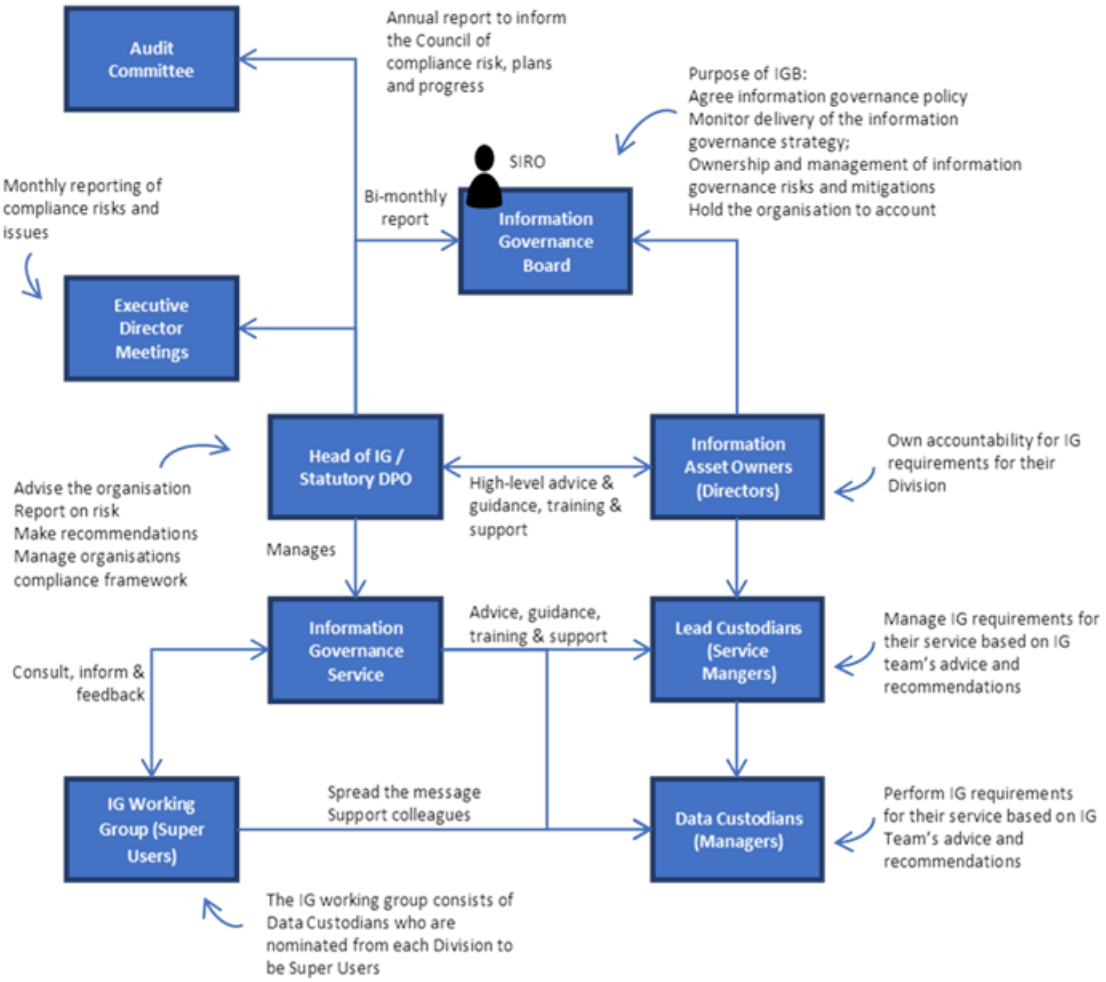
Lead Custodians – Lead Custodians are BCC's Service Managers and they have responsibility for managing the information being created, received or obtained by their service areas. Their responsibilities are similar to Information Asset Owners within their own service areas.

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 MANAGEMENT

The management of Information Risk is carried out in accordance with the Council's Risk Management Framework. This is an established framework for the management of risk across the Council.

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.

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. Full details of the Corporate Risk Register entries relating to information risk, including risk scoring and mitigations are reported separately to the Audit Committee and to Cabinet on a quarterly basis.

The Council's Risk Management Framework is also used for the management of Corporate Risks. The Corporate Risk register contains 3 risks relating to information risk: CRR7: Cyber-Security; CRR25: Suitability of Line of Business systems; and CRR29: Information Security Management System, all of which are currently scored as 20 under the Council's Risk Management Framework. The following actions have been taken to manage and mitigate these risks.

CRR7: Cyber Security – Given the ever-changing cyber security landscape and the types of vulnerabilities and threats, this remains a high risk to the Council, as it is to any large organisation. However, a significant amount of work has been carried out to manage this risk. There has been investment in technical controls to reduce the threat to the Council from cyber-attacks and this will need to continue.

CRR25: Suitability of Line of Business systems – The prevalence of legacy systems within the Council is an ongoing risk. A formal review of Line of Business systems has been initiated which will identify gaps which will require remediation.

CRR29: Information Security Management System – It remains a significant risk to the Council to not have in place an effective Information Security Management System. Work has continued to implement an Information Security Management System, including the roll out of updated policies and training for staff.

The effective management of risk requires up-to-date information, professional advice and support and the sign-off of risk at an appropriate level. Most risks are managed and mitigated through dialogue with Service Teams and following advice from the Information Governance Service and the IT Service. However, it is sometimes necessary for risks to be escalated to the SIRO. In particular this will be the case where a risk relates to one of the Corporate Risks and the Service Team is not in a position to mitigate the risk in the short to medium term. Following advice from the Information Governance Service and the IT Service, the SIRO is able to authorise an exception for a period of time to enable further work to be done to identify mitigations and an appropriate timeline for action. In taking any decision to authorise an exception, it is necessary for the SIRO to balance the needs of the business against the identified risk. Exceptions that have been approved by the SIRO are kept under review and will be reported to the Information Governance Board.

4. KEY DELIVERABLES OVER THE LAST 12 MONTHS

The SIRO Assurance report that was presented to the Audit Committee in September 2020 highlighted a number of activities that would be progressed over the following 12 months. The following key deliverables have been achieved during the last 12 months.

- Information Governance Board – established in April 2019, the Information Governance Board continues to meet monthly, to have oversight of the Information Risk management policies and procedures within the Council. 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. The Information Governance Board is an important assurance mechanism for the SIRO and this Board has carried out a number of important assurance functions over the last 12 months, including

the approval of applications for external certification, approval of the first suite of policies that will form part of the Information Security Management System, review of Internal Audit reports relating to information risks, oversight of corporate risk mitigations and an escalation point for emerging risks and SIRO exception reporting.

- Head of Information Assurance – following the appointment of a permanent Head of Information Assurance in September 2019, the Information Management, Data Protection and Information Security agendas have become embedded in core management structures, for example with regular reporting to Directorate Management meetings. The Customer Relations Team (responsible for complaints, FOIs and DP requests) as well as the Modern Records Team (responsible for archived information management) have also been brought into this service area which will create consistency in the Council's approach to information management.
- Information Security Management System – work which began in November 2019 has continued to implement an Information Security Management System. This is a series of policies and procedures designed to align with ISO 27001 for the effective and robust management of Information Risk. A significant part of this work has been the collation of all Information Risks within the Council (encompassing Information Security risks as well as Data Protection risks). The Council is then able to apply the risk management framework to identify mitigations for these risks. A number of key policies that are applicable to all staff have been refreshed as part of this work, including Acceptable User, Agile Working, Access Control (both logical and Physical) as well as Training and Development procedures.
- IT Transformation Programme – the Information Governance Service continued to support the ITTP programme to ensure that good information governance is embedded in the IT transformation work. Whilst the ITTP has now concluded, the Information Governance Service will continue to support the next programme of activity under Digital Transformation Governance Board.
- GDPR Phase II Project – The General Data Protection Regulation Phase II project commenced in October 2020 with the approval of an outline business case. The project 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.
- Information Management Strategy – Through the Council's Data Insights Assurance Board ("DIAB"), an information Management Strategy has been developed. This strategy sets out how the Council plans to use its data assets in a legal and ethically compliant manner, whilst also ensuring we use data to improve services, anticipate future demand and undertake data-led decisions. Effective governance will ensure that all data, wherever it is held, is used appropriately and safely.
- External Certification – the Council has continued to maintain the required assurance certifications, such as PSN and NHS Toolkit. The Council has also obtained certification from the Governance and Risk Return (GIRR) for the Police. All these processes for external certification involve submitting evidence to the supervising Government body to show we comply with their requirements. Work has also commenced on Cyber Essentials, a

government certification overseen by the National Cyber Security Centre and regarded as a key indicator of assurance.

- Training – Executive level training has been provided to senior leadership in June 2021 and a business continuity exercise with a focus on IT resilience has been carried out. Mandatory Information Security training and Data Protection training for all BCC continues to be delivered as part of the induction process and annual refresher training is prompted through the online training platform.
- A Caldicott Plan has been drafted setting out the roles and responsibilities of the Caldicott function within BCC. A Caldicott log which details matters of relevance to the processing of health and social care data, is maintained on the Caldicott's behalf by the Information Governance Service to ensure the Caldicott is involved and advised of matters pertaining to the processing of service user confidential data. A quarterly report is produced to the Caldicott detailing significant data sharing initiatives, privacy impact assessments and data breaches.

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.

- An Information Governance Strategy/Framework will be developed as part of the GDPR phase II project.
- The work to embed an Information Security Management System, including the roll out of more policies and training will continue. An assessment of the Council's preparedness to seek ISO27001 accreditation will be planned with a look towards a full roadmap for certification.
- The Information Governance Team will support Data Custodians to progress the remediation activity as identified in their risk mitigation plans. Further remediation work and internal audit activity will support this.
- Management actions relating to cyber security risks arising from recent internal audit work will be carried out. This will include a review of this Corporate Risk.
- The General Data Protection Regulation Phase II project, which commenced in October 2020 will be progressed through to Full Business Case stage. The project has its own governance structure with a Project Board and programme management support. It also provides monthly updates on progress to the Information Governance Board.
- The Council will continue to maintain external certification, e.g., PSN, NHS Toolkit, GIRR. In addition, the Council will be working towards Cyber Essentials assurance, and Cyber Essentials Plus assurance.
- The Common Activities programme will review the service delivery models for Freedom of Information and Data Protection within the Council.
- The information governance agenda will continue to be supported by an Internal Audit Programme of assurance work.
- Digital Transformation Governance Board – A new Governance and Assurance Board has been instigated to give oversight of all activities pertaining to Data & Insights, IT, Digital and Digital Place/Smart Cities. Information Assurance forms part of the governance remit and

provides an effective platform to raise concerns and seek appropriate senior leadership guidance to innovation activities.

- Further Business Continuity exercises relating to a Cyber Security incident will be carried out building on the business continuity exercise that was carried out in the previous 12 months.
- Further embed the role of the Caldicott Guardian within BCC to ensure processing of health and social care data is both lawful and ethical.
- The IT Transformation Programme (ITTP) has given the Council access to several new controls and approaches to help improve GDPR compliance and minimise Cyber threats. Information Assurance colleagues will evaluate and request the implementation controls on an on-going basis, and then monitor the effectiveness of the controls.

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 range of activity undertaken over the last 12 months enables the SIRO to provide assurance to the Audit Committee that a significant amount of work is being carried out within the Council to embed appropriate procedures to manage information risk.

It should be recognised that cyber threats continue to evolve, and the Council will always carry an element of risk regardless of investments in information assurance resources, training and awareness, and/or technical controls. By implementing a robust approach to risk management, creating an effective cross-Council approach to mitigating risks and ensuring that this remains high on the Council's agenda with appropriate investment in technical controls, we minimise our chances of being a victim of cyber threats and increase our chances of minimising losses/disruption, alongside formal review of the Information Commissioners Office.

The assurance framework that informs this report considers the 3 lines of defence:

The first line of defence considers the policies and procedures that are in place, for example, training, 'phishing' exercises and technical controls.

The second line of defence considers the oversight functions that are in place, for example, risk identification and monitoring by the Information Governance Service, oversight from the Statutory Data Protection Officer, reporting and monitoring of data breaches/cyber incidents by EDMs and oversight from the Information Governance Board.

The third line of defence considers the assurances received from Internal Audit reports, external assurances/certifications and learning from data breach/cyber security incidents.

With the three lines of defence in mind, the following actions provide the SIRO with assurance in respect of the management of Information Risk within Bristol City Council.

- Work of Information Governance Board – As highlighted in section 4 above, the work of the Information Governance Board is an important layer of assurance in the management of Information Risk. Over the last 12 months, the Information Governance Board has approved

applications for external certification, approved the first suite of policies that will form part of the Information Security Management System, reviewed Internal Audit reports relating to information risks, maintained oversight of corporate risk mitigations and been an escalation point for emerging risks and SIRO exception reporting.

- Work of Internal Audit – The embedded assurance role of the Internal Audit Service within the work of the Information Governance Board is very effective. It provides a range of support through the Internal Audit work programme and relevant information risk audits are regularly considered by the Information Governance Board. The following Internal Audit reports have been kept under review by the Information Governance Board, for example Data Privacy Impact Assessments, GDPR compliance and Cyber Security.
- Work of Information Governance Team, including escalation of risks to SIRO.
- Roll out of Information Security Management System – intention to achieve ISO 27001 accreditation
- 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.
- External assurance – PSN, NHS Toolkit, GIRR accreditations.
- Technical cyber controls – The Council has implemented a number of technical controls to automate the identification and removal of Information Security threats from the Councils software systems, computers and network.
- Training and Awareness continues to educate and empower colleagues to operate in a safe manner and be aware of Cyber risks and threats
- Managed Phishing exercises with follow up awareness.
- Data Protection and Information Security mandatory training.
- Business continuity exercise relating to cyber security.

7. CONCLUSION

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 progressed over the last 12 months to develop a more robust approach to the effective management of 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 embed key policies and procedures ensure that systems and processes are fully embedded at all levels within the Council.