1. Audit Summary – Cyber Security Review

Background and Context

1.1 Cyber risks are on the increase as the threat level has risen as a direct result of Covid-19. The World Health organisation has stated that cyber risks during the pandemic are fivefold what they were in February 2020. Bristol City Council identifies cyber security as one of the high-risk areas in its corporate risk register.

1.2 Local authorities hold critical information in the form of residents/customers' personal data, management/ financial information and staff payroll/HR information. Any data breaches will have a direct impact on the reputation of the Council in addition to any financial penalties imposed through legislative or contractual obligations. The Council therefore need to implement the appropriate technical, people and process related controls to be able to identify, mitigate and respond to cyber risks and breaches.

Scope and Objectives

1.3 In supporting the Information Governance Board, the objective of this audit was to review the design and implementation of cyber security controls in place across the Council to independently assess cyber maturity. The audit aimed to provide an independent opinion on how effectively the risks associated with cyber security are being managed and ensure processes are in place and operating to a standard that provides assurance in the following areas:

- **Leadership and Governance** – assessing the design and implementation of controls in place regarding the understanding of cyber risks, leadership roles and responsibilities and policy documentation
- **Risk Management** – assessing the information risk management policies and controls in place to manage information sharing across the business and third parties;
- **Security Operations and Technical Controls** – assessing the design and implementation of the technical controls in place to minimise cyber threats
- **Human Factors –** assessing the controls regarding IT security training and awareness, identification and management of specialist skills with regards to security and training needs analysis for security professionals.

Audit Opinion

1.4 Overall, Internal audit obtained **limited assurance** that effective internal control and risk management measures were in place.

Key Messages and Findings:

1.5 The Council has established an Information Governance Board which has overall responsibility for Cyber Security. Recent investment has been made in tools/systems to enhance the security posture of the Council. Health checks and regular penetration testing are carried out and technical security solutions are installed to help protect networks and newly deployed devices. In 2019, the council started work to implement an Information Security Management System (ISMS) which will, once implemented, provide a framework for information security management system that is aligned to ISO 27001. Areas for improvement were identified as follows:

<u>Leadership and Governance:</u>

1.6 An information security or cyber security strategy was not in place to establish the council's short and longer term cyber security aims and plan how these will be achieved. Without such a strategy, the Council may not be able to prioritise proactive investment in cyber security measures required.

1.7 A number of information security policies and operational procedures are either not yet finalised or are in place but have not been regularly reviewed. There is no schedule to ensure that policies or operational procedures are reviewed at regular intervals to ensure they are up to date.

Risk Management

1.8 Documentation around the risk management framework is in place but is yet to be finalised. There is no defined information security risk appetite, the operational risk register needs refining and a formal process to report regular security updates to the Information Governance Board needs to be established.

1.9 Whilst an information asset register is in place, fields are not consistently completed and the roles and responsibilities of information asset owners in managing risks are not clear. In some cases, information asset owners were not recorded leaving accountability for information assets unclear.

Security Operations and Technical Control:

1.10 Security operations roles and responsibilities are not clear which could lead to non-completion of routine security tasks.

1.11 A large number of applications are managed outside Central IT, as such the IG Team, responsible for information security, does not have visibility over the application.

1.12 Some key technical controls and polices require further improvements.

1.13 User access management processes require work to ensure the processes are appropriately managed in a timely manner.

1.14 Use of encrypted USB drives for transfer of data is not enforced on windows 7 devices. New device rollout is ongoing and hence this risk has been accepted in the short term whilst the roll out is competed.

Human Factor:

1.15 All staff are required to undertake mandatory training in relation to information security and completion rates are monitored by the Information Governance Team. A formal training needs analysis has not been completed and would support identification of specific training needs to enhance cyber awareness across the Council.

Management Response

1.16 The report has been well received by management who have agreed a number of improvement actions. Implementation is being monitored by the Information Governance Board.

1.17 All actions are being addressed, with some already completed (such as policies) and the large majority already underway.

1.18 Certain actions are more challenging to address; however, Information Governance colleagues are working closely with IT colleagues to ensure the appropriate actions are carried out.

1.19 The majority of actions will be closed out by the end of the calendar year, with a small number rolling into next year.