Report to Audit Committee

Senior Information Risk Owner Review for the Financial Year 2021/22

Portfolio Holder: Councillor Abdul Jabbar MBE – Deputy Leader and Cabinet Member Finance and Low Carbon

Officer Contact: Anne Ryans - Director of Finance

Report Author: Mark Stenson – Assistant Director of Corporate Governance and Strategic Financial Management

9 June 2022

Purpose of Report

To update Members of the Audit Committee on information security breaches, risk issues / actions.

Executive Summary

This is the annual report of the Senior Information Risk Owner (SIRO) to the Audit Committee highlighting Information Security Incidents and related matters which have occurred throughout 2021/22.

Recommendations to the Audit Committee

The Audit Committee is asked to note the content of the report.

Senior Information Risk Owner Review for the Financial Year 2021/22

1 Background

1.1 The Cabinet Office Data Handling Review in 2008 led to a requirement for NHS organisations and Local Authorities (as public sector bodies) to assign the role of the Senior Information Risk Owner (SIRO), a board level executive with particular responsibility for information risk.

1.2 The SIRO has responsibility for understanding how the strategic business goals of the organisation may be impacted by any information risks and for taking steps to mitigate those risks.

1.3 At the same time, there is a clear need to ensure that the Council's Caldicott Guardian works closely with the SIRO and that the Caldicott Guardian is appropriately consulted when information risk reviews are conducted for assets which are / or contain personal information.

1.4 A Caldicott Guardian's activity is particularly concerned with the seven Caldicott principles and the common law duty of confidentiality, whilst the SIRO is mainly involved in ensuring compliance with the Data Protection Act and other relevant legislation.

1.5 The SIRO is required to register with NHS Digital as Council access is required to national NHS IT systems or services.

1.6 The National Cyber Security Centre (NCSC) is an organisation of the United Kingdom Government that provides advice and support for the public and private sector in how to avoid computer security threats. Following international matters, the NCSC continues to call on organisations in the UK to bolster their online defences. While the NCSC is not aware of any current specific threats to UK organisations in relation to events in and around Ukraine, there has been a historical pattern of cyber-attacks against Ukraine with international consequences. The Council is implementing measures in line with NCSC recommended actions to take when the cyber threat is heightened.

2 Role Overview

2.1 The SIRO is responsible for owning the overall information risk policy and ensuring its effective use in the organisation, and for leading the cultural change necessary within the organisation to ensure information is valued, protected, and used properly by all members of staff, elected members, contractors / agency staff etc.

2.2 Within the Council, the SIRO:

- has overall ownership of the Council's Information Risk Policy;
- is required to act as champion for information risk to the Management Board and other leadership boards;
- is responsible for providing written advice to the Audit Committee on the content of the Council's Statement of Internal Control regarding information risk; and
- is responsible for decisions in relation to any information issues or incidents.

2.3 When security incidents involving personal data occur, the SIRO is a key stakeholder in determining whether the Information Commissioners Office (ICO), who is the regulator of the Data Protection Act, should be informed.

3 Responsibilities

3.1 The SIRO is expected to:

- acquire a knowledge of information risk management and its benefits;
- help develop the information risk management strategy and communicate it to senior management and elected members;
- promote and oversee the implementation of the strategy across the organisation;
- assist in monitoring and reviewing the information risk management strategy;
- agree any inputs and resources necessary to support the implementation of the strategy corporately; and
- assess and agree identified risks that are considered in line with the Council's risk appetite.

4 Information Governance Risk Management Policy

4.1 The Council has an Information Risk Management Policy. The policy identifies the roles and responsibilities at various levels including the SIRO.

4.2 The policy requires for the identification and management of information risks in a consistent, holistic way across the Council and focusses on information risks that, because of their likelihood and impact, make them management priorities.

5 Current Position

5.1 The Council has a SIRO in place.

5.2 The position of SIRO is held by Anne Ryans, Director of Finance with Mark Stenson, Assistant Director of Corporate Governance and Strategic Financial Management acting as Deputy SIRO.

5.3 The SIRO responsibilities extend to cover the MioCare Group Community Interest Community and the Unity Partnership Ltd (during 2021/22) under the service level agreements in place with the Council's Information Management Team.

5.4 Operational day to day responsibilities for the management and reporting of information risk, and information security breaches, rests with the Information Management Team.

6 Information Security Incidents

6.1 There were 80 information security incidents during 2021/22, compared to 68 during 2020/21. It is likely that number of incidents in 2020/21 reduced due to the coronavirus pandemic as during 2019/20 there were 103 incidents. Incidents during 2020/21 and 2021/22 are summarised in the table in Appendix 1.

6.2 The Caldicott Guardian is a senior role in an organisation which processes health and social care personal data. The duty of the Guardian is to ensure that personal data is used legally, ethically and appropriately, and that confidentiality is maintained. The Council has 2 Caldicott Guardians, 1 for Children's Services and 1 for Community Health & Adult Social Care.

6.3 The Information Management Team have worked with both Caldicott Guardian's to raise awareness, provide training, and issue key messages to staff. Furthermore, the Information Management Team and the Children's Caldicott Guardian analysed trends across the incidents and issued specific guidance to staff relating to how to minimise the risk of information being disclosed in error or shared inappropriately due to redaction issues.

6.4 Cyber-criminals continue to be an increased risk particularly around sending 'phishing' emails with the aim of getting users to click on a malicious link. It is important to remember that a single malicious link could lead to a successful attack, which could in turn compromise the IT network and put all information at risk. Reminders have been sent to all employees and Councilors requesting completion of the Council's interactive Mandatory Cyber Security training course. Cyber awareness guidance has also been added to the Council intranet and circulated to all staff. To further reduce risk, further work is being carried out to heighten awareness of phishing emails.

6.4 Cyber criminals target employees of organisations in order gain unauthorised access, infiltrate the network and compromise data, Local Authorities are popular targets. To reduce the risk, the Council successfully changed its policy on password complexity to align with the recommendations of the National Cyber Security Centre (NCSC). External independent validation has shown an improvement in the Council's password posture.

6.5 All software, including device operating systems, will eventually become out of date. The use of products which no longer receive security updates and where the latest security mitigations are not present make high impact incidents more likely. Work is being undertaken across the Information Management Team and IT to implement a policy and system to reduce the likelihood and impact of compromise of legacy systems In line with NCSC recommendations.

7 Security Standards

Public Services Network (PSN) Accreditation & Compliance

7.1 The PSN is a secure network that allows local and national public sector organisations to interact and share data privately and securely. On an annual basis the Council is required to obtain certification for the forthcoming year. The Information Management Team, working with ICT Services, manage the annual PSN certification submission. The current certification runs to the 26 March 2023.

Data Security & Protection Toolkit Accreditation & Compliance

7.3 The submission of the Council's Data Security and Protection Toolkit (DSPT) annual mandatory assessment was made by the end of June 2021, with a partial submission, with one outstanding area – training. This was completed within the timescales agreed and a full submission was presented.

7.4 The Council is preparing for the 2022 submission which will be completed by the end of June. There remains a risk that a partial submission may need to be submitted due to training requirements, services are working together to reduce this risk prior to the submission deadline.

8 Consultation

8.1 Officers of the Council have been consulted in the preparation of this report.

9 Financial Implications

9.1 N/A

10 Legal Services Comments

10.1 N/A

11 Co-operative Agenda

11.1 Committed to the Borough - to visibly demonstrate that the Council is taking steps to ensure legal compliance and manage its risks accordingly.

12 Human Resources Comments

12.1 N/A

13 Risk Assessments

13.1 N/A

14 IT Implications

14.1 N/A

15 Property Implications

15.1 N/A

16 Procurement Implications

16.1 N/A

17 Environmental and Health & Safety Implications

17.1 N/A

18 Equality, community cohesion and crime implications

18.1 N/A

19 Equality Impact Assessment Completed?

19.1 N/A

20 Key Decision

20.1 No

21 Key Decision Reference

21.1 N/A

22 Background Papers

24.1 The following is a list of background papers on which this report is based in accordance with the requirements of Section 100(1) of the Local Government Act 1972. It does not include documents which would disclose exempt or confidential information as defined by the Act:

File Ref:	Background papers are included as Appendices
Officer Name:	Victoria Gallacher
Contact No:	Extension 8488

25 Appendices

25.1 Appendix 1 – Information Security Breaches by Directorate

Appendix 1 - Information Security Breaches by Directorate

Directorate	Quarter 1	Quarter 1	Quarter 2	Quarter 2	Quarter 3	Quarter 3	Quarter 4	Quarter 4	Total by Service
	Apr-Jun 20-21	Apr-Jun 21-22	Jul-Sept 20-21	Jul-Sept 21-22	Oct-Dec 20-21	Oct-Dec 21-22	Jan-Mar 20-21	Jan-Mar 21-22	
Chief Executive & Legal Services	1	0	2	2	2	2	0	1	10
Children’s Services	3	9	6	8	9	6	7	6	54
Commissioning	0	4	2	6	2	1	2	4	21
Community Health & Adult Social Care	3	3	4	5	3		1	5	24
People and Place	2	4	1	2	4	1	3	1	18
Communities & Reform	1	1	1	2	1	3	1	2	12
Others	1	0	2	1	2	0	2	1	9
Total (2020-21)	**11**	**-**	**18**	**-**	**23**		**16**		**68**
Total (2021-22)	**-**	**21**	**-**	**26**	**-**	**13**	**-**	**20**	**80**

***Reported in line with the Management Structure in place for the financial year 2020/21 and the first part of the financial year 2021/22 (for comparison purposes)**

Incidents can be categorised as follows:

Incident Type	2020/21	2021/22
Instances of information being disclosed in error	30	47
Instances of stolen / lost / misplaced records or equipment	3	8
Instances of technical failure	3	9
Instances of unauthorised access/disclosure	25	13
Instances of uploading to a website/system in error	2	2
Minor issues	5	1
Total	**68**	**80**