Audit Committee

30 May 2023

Report of: Director of Legal and Democratic Services – Senior Information Risk Owner

Title: Senior Information Risk Owner Update

Ward: n/a

Recommendation

That the Committee notes the contents of this report.

Summary

This report provides an overview of the assurances that the Council's Senior Information Risk Owner has received in respect of the Council's management of information risk.

The significant issues in the report are:

As set out in the report.

Policy

1. In September 2021, the Senior Information Risk Owner (SIRO) reported on the matters that were being progressed to strengthen the Council's management of information risk. In September 2021, the foundations of good information risk management were in place, however, it was recognised that further improvements were required in certain areas.

This report provides an overview of the sources of assurance for the SIRO, actions that have taken place since September 2021 to improve the Council's management of information risk, and a look ahead to areas for further action over the next year.

Consultation

2. Internal
Chief Internal Auditor; Head of Information Assurance.

3. External
Not applicable.

Background

4. The SIRO is the senior officer at the Council with overall responsibility for Information Risk and who has responsibility for sponsoring and promoting Information Governance policy within the Council.

5. The SIRO provides assurance to the Council as part of the Annual Governance Statement, which includes the following comment in respect of information risk:

"Policies and processes are in place for the management of information governance risks. The Information Governance Team works to identify and manage cyber security risks. This remains a high risk for the Council due to the ever-changing nature of cyber threats. There is an escalation process for the approval of exceptions to information security policies, which is documented as part of the Risk Management Framework and risks will be escalated to the Senior Information Risk Owner as appropriate. The establishment of a centralised disclosures team this year brings together expertise to improve the robustness in approach across the Council to the effective management of data.

The Council's Senior Information Risk Officer has confirmed that there are no significant exceptions or breaches that have been identified in respect of compliance with the information security policies during 2022/23. An Internal Audit review of GDPR Compliance concluded reasonable assurance that controls are in place to support compliance by the Council."

Sources of assurance

6. The SIRO looks to the following areas of activity to obtain assurance about the Council's approach to the management of information security risk.

6.1. Information Governance Board

The arrangements relating to the Information Governance Board are well-established and there is cross-Council representation and embedded assurance from Internal Audit on this Board. Assurance mapping has been done to inform the work programme for the Board, with monthly reporting from the Head of Information Assurance and review of management actions relating to Internal Audit reports.

6.2. Data Protection

The Council's has appropriate arrangements in place to ensure compliance with data protection laws. In addition, the Council's arrangements for managing data protection duties have been strengthened by the centralisation of a Disclosures Team as part of Common Activities.

6.3. Information Asset Owners

Information Asset Owners are accountable for the information being created, received or obtained by their directorate. Recent Internal Audit work has identified that this remains an area for improvement and appropriate management action is required to ensure that the obligations and responsibilities of IAOs are understood and embedded within the Council.

6.4. Internal Audit work

There has been a significant amount of internal audit work to support the Council's information security activity since September 2021. The internal audit work has concluded that IT Asset Management, GDPR compliance and Ethical Use of Data are areas with a reasonable level of assurance. However, IT Resilience, IT governance, Cloud resilience, Core Systems Access Controls and Information Asset Ownership governance are all areas with a limited level of assurance and these have been reported to the Council with appropriate management plans identified.

In particular, there are a number of 'limited assurance' audit findings which require extensive management action. The report by the Director: Policy, Strategy and Digital to the Audit Committee in January 2023 set out a wide range of management action that would be taken forward to enhance IT governance and resilience.

6.5. External accreditation

To access data from third parties, it is necessary for the Council to meet minimum standards of security. The Council continues to maintain the following external accreditations: PSN, NHS and GIRR.

6.6. Where gaps have been identified above, these will inform future areas of internal audit activity and management action as set out in section 8 of this report.

Areas for improvement

7. In September 2021, the report to the Audit Committee identified a number of areas for improvement.

7.1. The following table sets out the areas of improvement that were identified in September 2021 and details of how these matters have been progressed.

Area for improvement	Progress
Development of an Information Governance Strategy/Framework	An Information Governance Strategy and an Information Governance Framework have been adopted
Embedding Information Security Management policies and training	A suite of Information Security Management policies has been prepared and mandatory training is in place. Further training will be developed on specific policies.
Remediation activity as identified in risk mitigation plans	The Information Governance Service continues to support service areas with the mitigation of information security risks
Progress management actions relating to cyber security audits	There are plans in place to progress management actions from cyber security audits as referenced elsewhere in this report
Progress of GDPR phase II project	This project has now been delivered
Maintaining external certification	The Council continues to maintain PSN, NHS and GIRR accreditation
Common Activities work	The Council has completed the Common Activities work to create a centralised Disclosures Team
Internal Audit work	There continues to be embedded assurance from Internal Audit at the Information Governance Board and a regular programme of internal audit activity. Internal Audit also provides embedded assurance at the Digital Transformation Programme Board
Information governance support to Digital Transformation	There continues to be appropriate representation and support from Information Governance at Digital Transformation Programme Board and relevant project boards
Cyber security business continuity exercise	Cyber security has been the subject of a business continuity exercise and further exercises are planned
Role of Caldicott Guardian	The Caldicott Guardian role is embedded within the Council's information governance arrangements
Use of IT controls to minimise cyber security threats	The Council continues to explore how to optimise relevant digital tools to combat cyber security threats

7.2. Where gaps have been identified above, these will inform future areas of internal audit activity and management action as set out in section 8 of this report.

Future Actions

8. As identified in the preceding sections of this report there remain some gaps and risks in relation to the management of information risk within the Council, which will require management action as well as Internal Audit activity.

9. The areas of management action have been identified as follows:

- Actions to enhance IT governance and resilience;
- Further training on specific information security management policies;
- Implement management action arising from cyber security audits;
- Further cyber security business continuity exercises;
- Optimising relevant digital tools to combat cyber security threats.

10. It is anticipated that Internal Audit activity will focus on the following areas:

- Records management;
- Cyber security;
- Disclosures Team processes;
- Information Asset Ownership – follow-up;
- Core Systems Access Controls – follow up; and
- Continued embedded assurance at the Information Governance Board.

Conclusion

11. The landscape relating to information risk management is ever-changing. The Council has made good progress to embed appropriate information risk management policies and procedures since September 2021. There remain areas for further on-going action. However, the risks are being appropriately managed.

Appendices:
None

LOCAL GOVERNMENT (ACCESS TO INFORMATION) ACT 1985
Background Papers:
None