



<b>Committee</b>	Audit and Governance Committee
<b>Date</b>	08/07/2024
<b>Subject</b>	Annual Senior Information Risk Owner Report
<b>Cabinet Member</b>	Councillor Paul Ashton, Deputy Leader and Cabinet Member with responsibility for Corporate Services (Digital, Customer Services, HR and Assets)
<b>Report Author and Head of Service</b>	Siobhan Martin Head of Internal Audit <a href="mailto:siobhan.martin@eastsuffolk.gov.uk">siobhan.martin@eastsuffolk.gov.uk</a>
<b>Director</b>	Chris Bally Chief Executive <a href="mailto:chris.bally@eastsuffolk.gov.uk">chris.bally@eastsuffolk.gov.uk</a>

Key Decision?	No
Is the report Open or Exempt?	OPEN

## Purpose/Summary

To review the annual Senior Information Risk Owner Report 2023/24.

This report presents Members with an overview of the Senior Information Risk Owners role within the Council, the governance measures and controls in place to protect the Council, work undertaken for the financial year from 2023/24 and priorities for 2024/25.

The activities detailed in the report have been carried out in line with and adhering to the legal obligations/statutory obligations under (not exhaustive):

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018.
- Freedom of Information Act (FOI) 2000
- Environmental Information Regulations (EIR) 2004
- Payment Card Industry Security Standard

The report is fundamental to demonstrate the Council's foundations of corporate governance, risk, and control.

This report has been prepared in accordance with the Audit and Governance Committee's terms of reference to: Review the effectiveness of the system for monitoring compliance with laws and regulations and the results of management's investigation and follow-up of any instances of non-compliance

## Recommendation(s)

That the Audit and Governance Committee:

1. Reviews and considers and comments on the annual Senior Information Risk Owner Report 2023/24.

## Strategic plan

How does this proposal support Our Direction 2028?

<b>Environmental Impact</b>	There are no environmental implications.
<b>Sustainable Housing</b>	There are no sustainable housing implications.
<b>Tackling Inequalities</b>	There are no inequalities implications.
<b>Thriving Economy</b>	The annual Senior Information Risk Owner Report directly links to the Council's framework of corporate governance, which encompasses the Council's strategic plan Our Direction 2028 and activities that support and enhance our thriving economy.
<b>Our Foundations / governance of the organisation</b>	<p>The annual Senior Information Risk Owner Report is an overview of the Senior Information Risk Owners role within the Council, the governance measures and controls in place to protect the Council, work undertaken for the financial year from 2023/24 and priorities for 2024/25.</p> <p>The core responsibility of the Senior Information Risk Owner is to provide the Corporate Leadership Team and Members with</p>

assurance that information risk is being managed appropriately and effectively across the organisation.

The entire annual Senior Information Risk Owner Report directly links to the Council's framework of corporate governance, which encompasses the Our Direction 2028. The report demonstrates the Council's adherence to its legal obligations, has appropriate structures, policies, guidance and processes in place to ensure the Council is able to manage its information securely and effectively. Identifying strengths and weaknesses thus improving the governance environment, supporting the Council's technical controls, over applications, information, infrastructure, and people, where applicable, which proactively contributes to delivering the Our Direction 2028.

## Justification for recommendations

### **1. Background**

- 1.1. Information is a vital asset to any organisation, and a large and complex organisation like East Suffolk Council holds and manages a vast amount of information, some of which can be classified as sensitive in nature. It is therefore vital that appropriate structures, policies, guidance and processes are in place to ensure the Council is able to manage this information securely and effectively.
- 1.2. Information Governance describes the holistic approach to managing, using and sharing information, and includes coverage around access to information, data quality, information management, information security and information sharing, data privacy and information governance legislative compliance.
- 1.3. The Senior Information Risk Owner (SIRO) has overall strategic responsibility and accountability for information risk across the organisation. A key responsibility for the SIRO is to provide the Corporate Leadership Team with assurance that information risk is being managed appropriately and effectively across the organisation. In East Suffolk Council, the SIRO role is designated to the Head of Internal Audit, and the SIRO is a member of the Corporate Leadership Team.

### **2. Introduction**

- 2.1. The annual Senior Information Risk Owner report is to be reviewed and considered by the Committee at its July meeting and demonstrates that appropriate structures, policies, guidance and processes are in place to ensure the Council is able to manage this information securely and effectively.

### **3. Proposal**

- 3.1. The annual Senior Information Risk Owner Report is required in order for the SIRO to provide confidence to the Members that information risk is being managed appropriately and effectively across the organisation.

### **4. Financial Implications**

- 4.1. Non-compliance with UK GDPR, Data Protection Act 2018, FOI, EIR and Payment Card Industry Security Standard could result in possible fines.

### **5. Legal Implications**

- 5.1. The UK GDPR, Data Protection Act 2018, FOI and EIR are legal frameworks which all organisations nationally must adhere to. The annual Senior Information Risk Owner Report demonstrates how the Council has met and is adhering to its legal obligations under the above pieces of legislation.
- 5.2. All actions completed in line with the above statutes are fundamental to support the Council's foundations of corporate governance, risk, and control.

## **6. Risk Implications**

- 6.1. Non-compliance with UK GDPR, the Data Protection Act 2018, FOI, EIR, Payment Card Industry Security Standard and Cyber Security measures could result in damage to citizens privacy, potential damage to the Council's reputation and fines by the ICO.

## **7. Options**

- 7.1. There are no options to be considered in relation to this report.

## **8. Recommendations**

- 8.1. That the Audit and Governance Committee reviews and considers and comments on the annual Senior Information Risk Owner Report 2023/24.

## **9. Reasons for Recommendations**

- 9.1. To ensure the Committee fulfils its terms of reference and supports the SIRO role and responsibilities.

## **10. Conclusions/Next Steps**

- 10.1. This report demonstrates the outputs and results in relation to SIRO activity in financial year 2023/24.
- 10.2. To deliver all connected plans to this report such as the Data Protection Plan 2024/25, FOI/EIR Plan 2024/25 and the Cyber 360 review action plan.

## Areas of consideration comments

### Section 151 Officer comments:

Not applicable

### Monitoring Officer comments:

Not applicable

### Equality, Diversity and Inclusion/EQIA:

Not applicable

### Safeguarding:

Not applicable

### Crime and Disorder:

Not applicable

### Corporate Services implications:

*(i.e., Legal, Finance, Procurement, Human Resources, Digital, Customer Services, Asset Management)*

#### Financial

The annual Senior Information Risk Owner report directly links to the Council's framework of corporate governance, which encompasses the Our Direction 2028 and activities that support the financial stability of the Council, where applicable.

#### Human Resources

The annual Senior Information Risk Owner report directly links to the Council's framework of corporate governance, which encompasses the Our Direction 2028 and activities that support Officers training and to support Human Resources with disciplinary's should the need arise relating to information governance risk and controls.

#### Digital

The annual Senior Information Risk Owner report directly links to the Council's framework of corporate governance, which encompasses the Our Direction 2028 and activities that support the Council's technical controls over applications, information, infrastructure, and people, where applicable.

#### Legal

The UK GDPR, Data Protection Act 2018, FOI and EIR are legal frameworks which all organisations nationally must adhere to. The annual Senior Information Risk Owner report demonstrates how the Council has met and is adhering to its legal obligations under the above pieces of legislation.

### Residents and Businesses consultation/consideration:

Not applicable

## Appendices:

<b>Appendix A</b>	Annual Senior Information Risk Owner Report 2023/24
-------------------	---

## Background reference papers:

Date	Type	Available From
------	------	----------------

2018	Data Protection Act 2018	HM Government
2018	UK General Data Protection Regulation	ICO
2000	Freedom of Information Act 2000	HM Government
2004	Environmental Information Regulations 2004	HM Government
2020	Our Direction 2028	Head of Internal Audit