

# North Lanarkshire Council Report

## Finance and Resources Committee

Does this report require to be approved?  Yes  No

Ref REB Date 04/03/26

## Senior Information Risk Owner (SIRO) – Information Governance – Assurance and Performance Interim Report

**From** Rachel Blair, Chief Officer (Legal and Democratic)

**E-mail** BlairR@northlan.gov.uk **Telephone**

### Executive Summary

This Senior Information Risk Owner (SIRO) report provides assurance to the Finance and Resources Committee that the Council's information governance, data protection and information security arrangements remain effective, proportionate and appropriately overseen. These arrangements support the Council in meeting its statutory, regulatory and good practice obligations, while protecting the confidentiality, integrity and availability of information essential to service delivery and public trust.

This report covers the interim period from January to March 2025. It has been prepared to close out reporting under the previous calendar-year SIRO reporting cycle and to support the transition to annual SIRO reporting aligned to the financial year (April to March), in line with other corporate governance, risk and assurance reports considered by Committee.

From April 2025, the statutory role of SIRO transferred from the Chief Officer (Business and Digital) to the Chief Officer (Legal and Democratic Services), following approval of governance changes through the *One Place, One Plan – Governance Update*. This change strengthens alignment between information governance, legal compliance and corporate assurance, and future SIRO reports will reflect this revised governance structure.

The primary purpose of this interim report is to:

- Provide clear, concise and proportionate assurance across the key areas for which the SIRO is accountable;
- Confirm whether any material changes to assurance positions arose during the January–March 2025 period; and
- Provide forward-looking context by summarising known improvements and developments being delivered during 2025/26, ensuring the report remains relevant when considered by Committee.

To support clarity and transparency, the report adopts a structured, assurance-based approach, presenting the Council's position through a single consolidated assurance table at Appendix 1. This approach avoids duplication with detailed operational reporting, strengthens the line of sight between assurance and risk, and enables Members to readily understand:

- What assurance was previously provided;
- Whether that assurance position has changed; and
- What further improvements are being delivered.

---

## Recommendations

It is recommended that Finance and Resources Committee:

- (1) Acknowledge the assurance provided by the SIRO in respect of the Council's information governance, data protection and information security arrangements for the period January to March 2025. ;
- (2) Acknowledge the transition to annual SIRO reporting on a financial-year basis from 2025/26 onwards;
- (3) Endorse the assurance-based reporting approach adopted within this interim report; and
- (4) Acknowledge that delivery of the Digital North Lanarkshire Programme of Work continues to provide a significant opportunity to strengthen information governance, cyber security and data management maturity during 2025/26.

---

## The Plan for North Lanarkshire

Priority	All priorities
Ambition statement	All ambition statements
Programme of Work	Statutory / corporate / service requirement

---

### 1. Background

- 1.1 Information governance and information security responsibilities are distributed across multiple officers, teams and governance structures within the Council. While specialist functions provide expertise and operational delivery, effective information governance relies on strong leadership, clear accountability, robust assurance mechanisms and consistent organisational compliance.
- 1.2 The SIRO acts as the Council's corporate champion for information governance, providing senior-level ownership of information risk and assurance to the Corporate Management Team and the Finance and Resources Committee. This includes oversight of compliance with data protection legislation, information security standards, records management obligations and associated risk management arrangements.
- 1.3 This report provides the SIRO's assessment of the Council's information governance arrangements for the period January to March 2025, representing an interim assurance position ahead of the move to annual financial-year SIRO reporting.

---

### 2. Report

- 2.1 The Council has well-established information governance, data protection and information security arrangements, embedded within its wider corporate governance, risk management and internal control framework. These arrangements are supported by documented policies and standards, technical controls, mandatory training, and structured governance oversight.

- 2.2 Oversight of information governance continues to be provided through the Data Governance Board (DGB), which monitors compliance, risk, incidents, improvement activity and assurance across the organisation. This is supported by specialist operational teams with responsibility for data protection, cyber security, records management and digital services.
- 2.3 Previous SIRO reports have confirmed that the Council operates at a developing level of data and information management maturity, with sustained and measurable improvement achieved over recent years. This has been driven by targeted investment in systems, strengthened governance, improved training compliance and increased senior oversight of information risk.
- 2.4 To improve transparency, readability and Member assurance, this interim report presents the SIRO's assurance through the consolidated assurance table at Appendix 1, covering the key statutory and good-practice areas relevant to the SIRO role. This includes data protection compliance, cyber security, incident management, risk management, records management, training and awareness, and corporate accountability.

## **Conclusion**

- 2.5 Based on the evidence reviewed, the SIRO is satisfied that appropriate and proportionate information governance, data protection and information security arrangements were in place during the period January to March 2025.
- 2.6 No material deterioration in assurance was identified during this interim period, and no regulatory enforcement action was taken against the Council.
- 2.7 The transition to financial-year SIRO reporting will enable stronger alignment with corporate planning, risk management, audit and digital transformation activity, and will allow future reports to provide a more comprehensive, outcome-focused and forward-looking assurance position.

---

## **3. Measures of success**

- 3.1 Effective information governance and information security support the Council in protecting services, finances and reputation.
- 3.2 Measures of success include:
- Continued compliance with statutory and regulatory requirements;
  - Sustained or improving assurance positions across all SIRO assurance areas;
  - Absence of significant regulatory enforcement or uncontrolled information risk; and
  - Demonstrable improvement in maturity, resilience and organisational awareness.

---

## **4. Supporting documentation**

- 4.1 Appendix 1 SIRO Assurance Summary – January to March 2025.



**Rachel Blair**  
**Chief Officer (Legal and Democratic)**

---

## 5. Impacts

<p><b>5.1 Public Sector Equality Duty and Fairer Scotland Duty</b> Does the report contain information that has an impact as a result of the Public Sector Equality Duty and/or Fairer Scotland Duty? Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> If Yes, please provide a brief summary of the impact?</p> <p>If Yes, has an assessment been carried out and published on the council's website? <a href="https://www.northlanarkshire.gov.uk/your-community/equalities/equality-and-fairer-scotland-duty-impact-assessments">https://www.northlanarkshire.gov.uk/your-community/equalities/equality-and-fairer-scotland-duty-impact-assessments</a> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/></p>
<p><b>5.2 Financial impact</b> Does the report contain any financial impacts? Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> If Yes, have all relevant financial impacts been discussed and agreed with Finance? Yes <input type="checkbox"/> No <input type="checkbox"/> If Yes, please provide a brief summary of the impact?</p>
<p><b>5.3 HR policy impact</b> Does the report contain any HR policy or procedure impacts? Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> If Yes, have all relevant HR impacts been discussed and agreed with People Resources? Yes <input type="checkbox"/> No <input type="checkbox"/> If Yes, please provide a brief summary of the impact?</p>
<p><b>5.4 Legal impact</b> Does the report contain any legal impacts (such as general legal matters, statutory considerations (including employment law considerations), or new legislation)? Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> If Yes, have all relevant legal impacts been discussed and agreed with Legal and Democratic? Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> If Yes, please provide a brief summary of the impact?</p> <p>This report has legal relevance in that it provides assurance regarding the Council's compliance with existing statutory and regulatory requirements relating to information governance, data protection, records management and information security. It confirms that appropriate arrangements were in place during the reporting period and that no regulatory enforcement action was taken, supporting the Council's ongoing compliance with its legal obligations.</p> <p>The report also reflects a governance change of legal significance through the formal transfer of the Senior Information Risk Owner role to the Chief Officer (Legal and Democratic Services), strengthening senior accountability for statutory information governance responsibilities. The report does not introduce new legal duties, employment law considerations or legislative changes, and is assurance-based in nature rather than proposing amendments to the Council's legal or policy framework.</p>

<p><b>5.5</b></p>	<p><b>Data protection impact</b>  Does the report / project / practice contain or involve the processing of personal data?  Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>  If Yes, is the processing of this personal data likely to result in a high risk to the data subject?  Yes <input type="checkbox"/> No <input type="checkbox"/>  If Yes, has a Data Protection Impact Assessment (DPIA) been carried out and e-mailed to <a href="mailto:dataprotection@northlan.gov.uk">dataprotection@northlan.gov.uk</a>  Yes <input type="checkbox"/> No <input type="checkbox"/></p>
<p><b>5.6</b></p>	<p><b>Technology / Digital impact</b>  Does the report contain information that has an impact on either technology, digital transformation, service redesign / business change processes, data management, or connectivity / broadband / Wi-Fi?  Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>  If Yes, please provide a brief summary of the impact?   Where the impact identifies a requirement for significant technology change, has an assessment been carried out (or is scheduled to be carried out) by the Enterprise Architecture Governance Group (EAGG)?  Yes <input type="checkbox"/> No <input type="checkbox"/></p>
<p><b>5.7</b></p>	<p><b>Environmental / Carbon impact</b>  Does the report / project / practice contain information that has an impact on any environmental or carbon matters?  Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>  If Yes, please provide a brief summary of the impact?</p>
<p><b>5.8</b></p>	<p><b>Communications impact</b>  Does the report contain any information that has an impact on the council's communications activities?  Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>  If Yes, please provide a brief summary of the impact?</p>
<p><b>5.9</b></p>	<p><b>Risk impact</b>  Is there a risk impact?  Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>  If Yes, please provide a brief summary of the key risks and potential impacts, highlighting where the risk(s) are assessed and recorded (e.g. Corporate or Service or Project Risk Registers), and how they are managed?  Yes. Information governance and information security present an ongoing corporate risk to the Council due to the potential impact of data breaches, cyber incidents or failures in statutory compliance, which could result in service disruption, financial loss, regulatory action and reputational damage. These risks are formally assessed and recorded within the Council's Corporate Risk Register as Information Governance and Information Security risks, with defined risk owners and agreed mitigating actions.   The risks are actively managed through established governance arrangements, including oversight by the Data Governance Board, implementation of technical and organisational controls, mandatory training and awareness activity, incident management processes, and regular assurance reporting to senior management and Committee. Progress against mitigation actions is monitored on an ongoing</p>

basis, with risks kept under review to ensure they remain within the Council's agreed risk appetite.

**5.10 Armed Forces Covenant Duty**

Does the report require to take due regard of the Armed Forces Covenant Duty (i.e. does it relate to healthcare, housing, or education services for in-Service or ex-Service personnel, or their families, or widow(er)s)?

Yes  No

If Yes, please provide a brief summary of the provision which has been made to ensure there has been appropriate consideration of the particular needs of the Armed Forces community to make sure that they do not face disadvantage compared to other citizens in the provision of public services.

**5.11 Children's rights and wellbeing impact**

Does the report contain any information regarding any council activity, service delivery, policy, or plan that has an impact on children and young people up to the age of 18, or on a specific group of these?

Yes  No

If Yes, please provide a brief summary of the impact and the provision that has been made to ensure there has been appropriate consideration of the relevant Articles from the United Nations Convention on the Rights of the Child (UNCRC).

If Yes, has a Children's Rights and Wellbeing Impact Assessment (CRWIA) been carried out?

Yes  No

**Appendix 1 – SIRO Assurance Summary – January to March 2025**

<b>Area of assurance</b>	<b>Assurance position as at February 2025 (covering January–December 2024)</b>	<b>Any subsequent update during January–March 2025</b>	<b>High-level summary of next steps being implemented during 2025/26</b>
<b>Data protection compliance</b>	Effective arrangements in place; no regulatory enforcement action by the Information Commissioners Office (ICO); breaches managed in line with statutory requirements.	Breach volumes comparable with the same period in 2024; no escalation to ICO enforcement.	Continued strengthening of accountability, privacy by design and Data Protection Impact Assessment (DPIA) processes; enhanced assurance reporting through annual SIRO report; continue to maintain and update data protection related registers; annual review of data sharing agreements.
<b>IT (cyber) security</b>	Compliance maintained with National Cyber Security Centre (NCSC) guidance, Public Services Network (PSN) and Payment Card Industry Data Security Standards (PCI DSS); no material cyber incidents.	No direct impact from national cyber incidents during this period; ongoing mitigation of known vulnerabilities.	Further modernisation of legacy systems through the Digital North Lanarkshire Programme of Work; enhanced vulnerability management and cloud security controls. Continue review of existing disaster recovery plans and processes; complete review of identification of critical systems; development of a corporate disaster recovery plan, and improved reporting and governance; improve and further develop connection of disaster recovery arrangements to business continuity and incident response arrangements.

Area of assurance	Assurance position as at February 2025 (covering January–December 2024)	Any subsequent update during January–March 2025	High-level summary of next steps being implemented during 2025/26
<b>Incident management</b>	Clear incident management processes in place; timely investigation and remediation of incidents.	Incident handling remained effective; lessons learned applied where appropriate.	Further integration of incident management with corporate risk and assurance reporting.
<b>Risk management</b>	Information governance and information security risks captured within the Corporate Risk Register with mitigating actions identified.	Residual risk position unchanged during this period.	Continued oversight by the Data Governance Board (DGB); alignment with refreshed corporate risk appetite and assurance framework.
<b>Records management</b>	Retention schedule in place and maintained; positive progress against actions agreed with the Keeper of the Records of Scotland.	Delivery of agreed actions continued as planned.	Completion of remaining improvement actions and further embedding of digital records management standards.
<b>Training and awareness</b>	Mandatory training compliance significantly improved and within green RAG thresholds.	Compliance levels maintained during this period.	Ongoing monitoring and targeted interventions; refreshed training content aligned to emerging risks.
<b>Information Asset Register</b>	Core Information Asset Register in place and maintained.	No material changes during this period.	Further maturity through improved ownership, assurance statements and integration with system lifecycle management.
<b>Information governance policies</b>	Policies and standards largely current and aligned to legislation and good practice.	Minor updates progressed as part of routine maintenance.	Planned policy refresh programme to align with updated operating model and digital transformation.

Area of assurance	Assurance position as at February 2025 (covering January–December 2024)	Any subsequent update during January–March 2025	High-level summary of next steps being implemented during 2025/26
<b>Corporate governance</b>	Information governance embedded within corporate governance arrangements and reporting.	Governance arrangements remained stable during this period.	Further alignment with One Place, One Plan governance model and committee reporting cycles.
<b>Accountability</b>	Clear roles defined for SIRO, Data Protection Officer (DPO), Information Asset Owners (IAOs) and operational teams.	SIRO role formally transitioned in April 2025.	Strengthened senior ownership and clearer escalation routes during 2025/26.
<b>Independent assessments / assurances</b>	Positive external assurance through PSN compliance and regulatory engagement.	PSN accreditation remained valid; no adverse findings.	Continued external assurance activity; preparation for future PSN and regulatory assessments.