North Lanarkshire Council
Report

Finance and Resources Committee

☐ approval ☒ noting **Ref** KH/RL/DGB **Date** 26/02/25

Senior Information Risk Owner (SIRO) – Information Governance – Assurance and Performance Report 2024

From Katrina Hassell, Chief Officer (Business & Digital)

Email HassellK@northlan.gov.uk **Telephone** 07903 096 121

Executive Summary

This Senior Information Risk Owner (SIRO) report aims to provide assurances that information risks are being effectively managed to ultimately enable the Council to comply with legislative requirements and good practice.

It summarises the Data Governance Board's (DGB) oversight of information governance arrangements for the period January to December 2024 and provides the SIRO's assessment of the Council's existing information governance and data accuracy arrangements. This report therefore outlines what is going well, highlights key matters of concern, and details the improvement actions which are required to be progressed – through the Data Management Team (DMT) – during 2025 to strengthen the Council's information governance arrangements.

Recommendations

It is recommended the Finance and Resources Committee:

(1) Acknowledge the activities which have been undertaken and/or are underway to enable the SIRO to provide assurance in respect of the Council's information governance.
(2) Endorse the areas of improvement which the SIRO has included within the live improvement plan for 2025.
(3) Recognise that progression of the Digital North Lanarkshire Programme of Work deliverable of '*ensure useful, secure, compliant and digital first applications are available to support critical but streamlined service delivery*' creates scope to significantly improve the Council's information governance and information security arrangements.

The Plan for North Lanarkshire

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

1. Background

1.1 There are several officers and teams across the Council with responsibility for information governance and information security, but good information governance involves everyone. This report describes how these roles collectively ensure organisational compliance with the legislative and regulatory requirements relating to the handling and processing of information.

1.2 As corporate champion for information governance, the SIRO aims to provide the Corporate Management Team and Finance and Resources Committee with assurances that information risks are being effectively managed. To this end, this report outlines information governance activity and performance in respect of the period January to December 2024. It provides the SIRO's assessment of existing arrangements, detailing what is going well, key matters of concern, and areas requiring further improvement and effort.

2. Report

2.1. The Council has always been committed to effective information governance with sound arrangements for ensuring compliance with legislation and recognised best practice appropriately managed as part of the Council's risk management and corporate governance arrangements.

2.2. The Chief Officer (Business and Digital) within the Chief Executive Office is presently the Council's Senior Information Risk Officer (SIRO), but following consideration of '*One Place, One Plan – Governance Update*' report at Policy and Strategy Committee in September 2024, this responsibility will transfer to the Chief Officer (Legal and Democratic Services) during 2025.

2.3. SIRO responsibilities include:

a) Leadership and overall ownership of the Council's Corporate Governance Action Plan, acting as corporate champion for information governance.
b) Acting as Executive Sponsor and advocate for the management of information governance at a senior level.
c) Providing advice and reports in respect of information incidents and risks, including the content of the council's Annual Governance Statement relating to information risk.
d) Owning the management of information governance and associated risk assessment processes within the Council.
e) Understanding how the strategic priorities of the Council may be impacted by information governance risks, and how these risks need to be managed including the adequacy of resources and levels of independent scrutiny.

2.4. Previous SIRO reports confirmed the Council operates effective information governance management arrangements, having undertaken and delivered significant technical and process improvements over recent years. Following on from the change implemented during 2023-2024, this annual SIRO report relates to the calendar year 2024, and therefore provides elected members with an up-to-date snapshot of current information governance management arrangements.

2.5. Sections 14 to 52 of the SIRO report provided as Appendix 1 detail performance and activity undertaken over the reporting period to ensure personal data is held securely, and information disseminated effectively. Key highlights for Committee consideration include:

- Information Security and Information Governance corporate risk monitored in accordance with residual risk ratings, with corresponding mitigating actions identified and deployed. (section 14 to 19)
- Reported data breaches are comparable with calendar year 2023, with improvements evident in the number of breaches reported to Legal Services within the required 72 hours. A higher percentage of breaches met the threshold for reporting to the Information Commissioner's Office (ICO), but the ICO did not apply any enforcement action or fines in respect of these. (section 20 to 27)
- The Council continues to follow published National Cyber Security Centre (NCSC) guidance, with several activities undertaken to mitigate against potential cyber security threats, including maintaining compliance with Public Sector Network (PSN) and

Payment Card Industry Data Security Standard (PCI DSS) requirements, fully deploying protection, preventative and detective tools, further developing information security standards, and transitioning all critical products to more secure and modern cloud-hosted solutions. (section 28 to 36)

- A re-assessment of the Council's Data Maturity Score during 2024 confirmed that delivery of improvement actions over recent years has resulted in the Council's maturity score improving from +1 (Initial/Basic) to -3 (Developing), an excellent achievement given the benchmark score for similar organisations is 2+ (Basic). (section 37 to 40)
- Increased oversight and monitoring of mandatory training activity has resulted in compliance levels vastly improving; for example, non-compliance as at 7th December for the Data Protection Essentials module ranges from only 2% for Chief Executives to 16% for Adult Health and Social Care. Members should note that non-compliance between 0% and 20% is RAG rated as Green. (section 41 to 48)
- Continued delivery of actions agreed with the Keeper of the Records of Scotland in respect of File Plan, Destruction Arrangements, Vital Records and Audit Trail. (section 49 to 52)

2.6. Complementing the Corporate Data Protection Officer's annual reports to the Finance and Resources Committee, sections 20 to 27 of the SIRO report, and Annexe B of the Appendix provide Committee with further details regarding data breaches identified during this reporting period, and the guidance and remedial actions applied following their assessment.

2.7. Sections 28 to 36 focus specifically on ICT Security and Cyber risks. These highlight the scale of the cyber security threat now facing all organisations and detail activities undertaken through Business and Digital to maintain a positive information governance assurance and mitigate against potential cyber risks. Paragraph 35 confirms that the Council was not affected directly by any notable cyber incidents during this reporting period.

2.8. Paragraphs 31(a), 33, 34 and 36 emphasise that addressing high-risk vulnerabilities in ageing critical systems is considered a key priority for 2025, with paragraph 58 confirming that actions are identified and largely underway through the approved Digital North Lanarkshire Programme of Work and capital investment programme to address this growing risk.

Next steps

2.9. The Council is committed to a clear strategy and sustainable framework for information governance and security, and effective data and information management governance is an essential component of that. Given this report presents information assurance for the 2024 calendar year, the live improvement plan detailed in section 54 of the Appendix highlights activity planned from January 2025 to strengthen existing arrangements.

2.10. By way of summary, the key priorities identified within the improvement plan include:

a. Raise the profile and prioritisation of Data Protection responsibilities.
b. Refresh and strengthen approach to mitigating cyber security risks and vulnerabilities.
c. Iterative deployment of the Data Governance Board approved workplan (Annex E).
d. Enhanced implementation of the Council's strategic approach to data and information management in line with the Programme of Work to 2028.

2.11 Improvements can always be made to our information governance arrangements, and with a residual risk score of 20 (October 2024) prevalent in respect of our Information Governance and Information Security corporate risk, it is essential this subject matter remains as a high priority improvement area for the Council. Progress against these key next steps will be managed by the DGB, who will look to further develop policies, guidance, standards, processes, and approaches as appropriate to improve awareness, understanding and compliance with legislative requirements and good practice.

3. Measures of success

3.1 Effective Information Security and Information Governance assists the Council in protecting itself from cyber-attacks and security breaches, which can both give rise to service delivery and financial pressures. Measures of success therefore flow from demonstrated and continued compliance with all information governance legislative and regulatory requirements.

---

4. Supporting documents

4.1 Appendix 1 – SIRO Information governance – assurance & performance – January to December 2024 Report.

Katrina Hassell
Chief Officer (Business & Digital)

5. Impacts (http://connect/report-template-guidance)

5.1 Public Sector Equality Duty and Fairer Scotland Duty

Does the report contain information that has an impact as a result of the Public Sector Equality Duty and/or Fairer Scotland Duty?

Yes ☐ No ☒

If Yes, please provide a brief summary of the impact?

If Yes, has an assessment been carried out and published on the council's website?

Yes ☐ No ☐

5.2 Financial impact

Does the report contain any financial impacts?

Yes ☐ No ☒

There are no immediate financial implications arising from this report; however, the promotion and implementation of effective information governance impacts positively on the Council's ability to mitigate its exposure to financial risk, particularly monetary penalties levied by the Information Commissioner's Office for non-compliance. Notwithstanding this, sections 31(a), 33, 34, 36, 54(b), and 58 of the SIRO report so appended illustrate action is required through available capital resources to ensure continued achievement with PSN accreditation and compliance with good practice standards.

If Yes, have all relevant financial impacts have been discussed and agreed with Financial Solutions?

Yes ☒ No ☐

If Yes, please provide a brief summary of the impact?

5.3 HR policy impact

Does the report contain any HR policy or procedure impacts?

Yes ☐ No ☒

If Yes, have all relevant HR impacts have been discussed and agreed with People and Organisational Development?

Yes ☐ No ☐

If Yes, please provide a brief summary of the impact?

5.4 Legal impact

Does the report contain any legal impacts (such as general legal matters, statutory considerations (including employment law considerations), or new legislation)?

Yes ☒ No ☐

Section 4 of the SIRO report as appended outlines the legislative and regulatory requirements placed on the Council in respect of information processing, security, and management. General Data Protection Regulations (GDPR) continue to apply to the United Kingdom post-Brexit implementation.

If Yes, have all relevant legal impacts have been discussed and agreed with Legal and Democratic Solutions?

Yes ☒ No ☐

If Yes, please provide a brief summary of the impact?

5.5 Data protection impact

Does the report / project / practice contain or involve the processing of personal data?

Yes ☒ No ☐

Section 4 of the SIRO report as appended outlines the legislative and regulatory requirements placed on the Council in respect of information processing, security, and management. General Data Protection Regulations (GDPR) continue to apply to the United Kingdom post-Brexit implementation. Paragraphs 20 to 27 also highlight any breaches of confidentiality and security considered by the DGB during the 2024 reporting period, with corresponding remedial actions identified.

If Yes, is the processing of this personal data likely to result in a high risk to the data subject?

Yes ☐ No ☒

If Yes, has a Data Protection Impact Assessment (DPIA) been carried out and e-mailed to dataprotection@northlan.gov.uk

Yes ☐ No ☐

5.6 Technology / Digital impact

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 ☒ No ☐

If Yes, please provide a brief summary of the impact?

Sections 28 to 36 of the SIRO report focus specifically on ICT Security and Cyber risks. Paragraph 30(c) provides context regarding the council's complex technology network, with paragraph 29 further highlighting the scale of the cyber security threat facing this complex network. The Digital North Lanarkshire Programme of Work creates scope to appropriately modernise and rationalise the Council's network, with resources prioritised in accordance with the risk assessments summarised within Annex C of the Appendix.

As referenced in paragraphs 2.8 and 5.2 above, addressing high-risk vulnerabilities in ageing critical systems is considered a key priority for 2025 to ensure the Council can maintain its PSN accreditation longer-term.

All changes required to maintain effective information governance and security will be considered by the appropriate corporate working group, with any technology components fully assessed when required by the corporate Enterprise Architecture Governance Group.

Where the impact identifies a requirement for technology, has an assessment been carried out (or scheduled) by the Enterprise Architecture Governance Group (EAGG)?

Yes ☒ No ☐

5.7 Environmental / Carbon impact

Does the report / project / practice contain information that has an impact on any environmental or carbon matters?

Yes ☐ No ☒

If Yes, please provide a brief summary of the impact?

5.8 Communications impact

Does the report contain any information that has an impact on the council's communications activities?

Yes ☒ No ☐

If Yes, please provide a brief summary of the impact?

Sections 6 and 54(a) of the SIRO report highlight that everyone – staff and elected members – must understand the importance of information governance and security. The live improvement plan continues to highlight a requirement for ongoing communication of requirements.

5.9 Risk impact

Is there a risk impact?

Yes ☒ No ☐

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?

In line with the Council's corporate risk management arrangements and a requirement for risk to be managed at an appropriate level of the organisation, the Chief Officer (Business & Digital) presently has lead officer responsibility for the corporate risk regarding Information Security and Information Governance. Approved risk management arrangements further require the assessment, monitoring, and review of individual risks to be assigned to relevant Corporate Working Groups, and this particular risk sits within the remit of the DGB.

The scale of the cyber security threat now facing all organisations sees the residual risk assessment of this corporate risk being retained at 20 "*almost certain*" likelihood (5) and "*major*" impact (4), with the likelihood of a breach considered high.

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

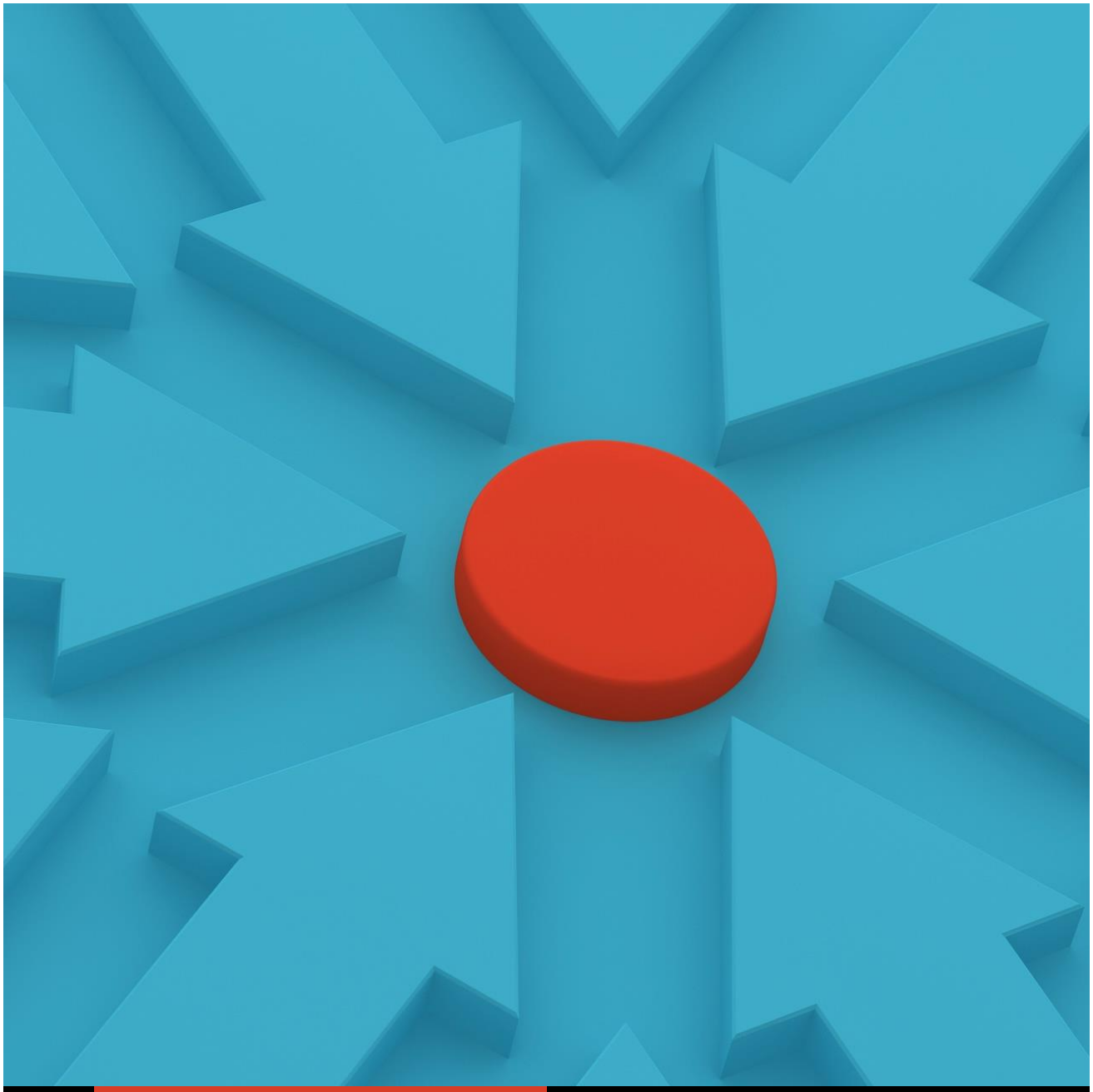
Does the report contain any information regarding any council activity, service delivery, policy, or plan that has an impact on children and young people up to the age of 18, or on a specific group of these?

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 ☒



SENIOR INFORMATION RISK OWNER (SIRO)

INFORMATION GOVERNANCE – ASSURANCE & PERFORMANCE: JANUARY TO DECEMBER REPORT

NORTH LANARKSHIRE COUNCIL December 2024

Table of Contents

EXECUTIVE SUMMARY

This report provides an update relating to the responsibilities of North Lanarkshire Council's Senior Information Risk Owner (SIRO). It outlines activity and performance related to information governance and provides assurances that information risks are being effectively managed. It outlines what is going well, any matters of concern, status of approved improvement actions, also indicating where further improvements can be made. This report relates to the period January to December 2024.

INTRODUCTION

1. The Senior Information Risk Owner (SIRO) Report reflects on the Council's information governance work, aiming to provide assurances that personal data is held securely, and information disseminated effectively. This report focuses on the period January to December 2024.

2. The Council continues to be committed to effective information governance, with sound arrangements in place to ensure compliance with legislation and recognised best practice. Governance arrangements are closely monitored to ensure systems, policies and procedures are fit for purpose, and that all staff and elected members understand the importance of information governance and security, with good practice considered everyone's business.

3. ICT security and cyber risks present an ever-increasing challenge to all organisations and the Council is no different. Arrangements to manage these risks, in consideration of the threat landscape, are contained within the report, with a summary included to highlight action underway and planned to maintain and strengthen defences and enhance corporate resilience.

4. Specifically, this report:

    a. Documents organisational compliance with the legislative and regulatory requirements relating to the handling and processing of information and provides assurance of ongoing improvements to manage information risks. This includes the Council's consideration and performance relating to:

        - Data Protection Act 2018 and General Data Protection Regulations (GDPR) 2016
        - Public Records (Scotland) Act 2011, and
        - Information Security Standard ISO/IEC 27001:2013
        - Managing data in line with the CIPFA Delivering good governance in local government framework

    b. Provides an overview of Council governance arrangements and key roles and responsibilities.

    c. Outlines any serious incidents which required investigation over the duration of this report, relating to any losses of personal data or breaches of confidentiality.

Key Roles and Responsibilities

5. The Chief Officer (Business and Digital) within the Chief Executive Office is presently the Council's Senior Information Risk Officer, but following consideration of '*One Place, One Plan – Governance Update*' report at Policy and Strategy Committee in September 2024, this responsibility will transfer to the Chief Officer (Legal and Democratic Services) during 2025. Key responsibilities include:

    a. Leadership and overall ownership of the Council's Corporate Governance Action Plan, acting as corporate champion for information governance.
    b. Acting as Executive Sponsor and advocate for the management of information governance at a senior level.
    c. Providing advice and reports in respect of information incidents and risks, including the content of the council's Annual Governance Statement relating to information risk.
    d. Owning the management of information governance and associated risk assessment processes within the Council.
    e. Understanding how the strategic priorities of the Council may be impacted by information governance risks, and how these risks need to be managed including the adequacy of resources and levels of independent scrutiny.

6. There are several officers and teams across the Council that have professional expertise relating to information governance and information security, but good information governance involves everyone. All staff and elected members therefore have personal responsibility to ensure information and data is held securely, processes appropriately and safely destroyed when not required.

7. Diagram 1 below illustrates existing responsibilities and governance arrangements in respect of information governance, clearly highlighting the differing responsibilities of the SIRO, Data Protection Officer, and Records Manager, as well as the oversight responsibilities of the strategic Data Governance Board (DGB) and operational Data Management Team (DMT).

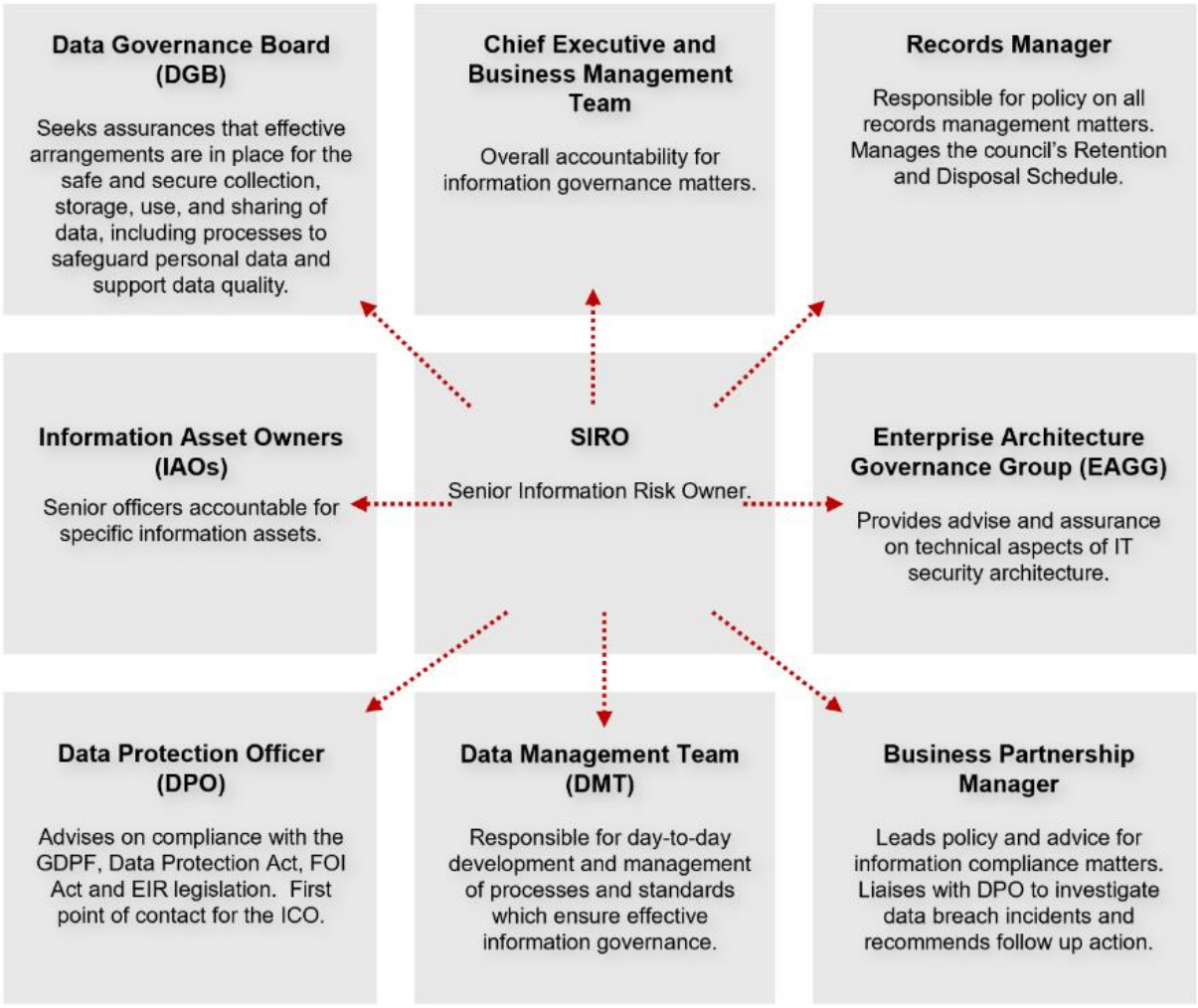


Diagram 1

8. Recognising these wider responsibilities, this report complements two annual reports prepared by the Chief Officer (Legal and Democratic Solutions) – the Corporate Data Protection Officer (DPO). The first report in respect of detailed 2023-24 responsibility for data sharing, data breaches, Information Commissioner Office (ICO) complaints was considered by the Finance & Resources Committee in September 2024. The second report detailing Freedom of Information (FOI) and Environmental Information Requests (EIR) for financial year 2023-24 is reported separately on today's agenda. This annual SIRO report provides additional context regarding data breaches, with details provided up to end of November 2024.

Governance and Monitoring Arrangements

9. The Council's Data Governance Board (DBG) is responsible for developing and implementing strategies, policies, and standards in relation to data governance and management. Additionally, the board is responsible for directing improvements identified in line with the data requirements of the council and its Programme of Work for 2023- 2028 and the DGB workplan (updated following the refresh, reframe, responsibilities review referenced in section 11 below), and for ensuring measures are in place, through the Data Management Team, to monitor compliance with approved policies and standards.

10. The DGB is presently chaired by the SIRO, includes the Corporate Records Manager, Data Protection Officer (DPO), the Strategy and Performance Manager, Chair of the Data Management Team (DMT) and key representation from all Council functions.

11. Although annual SIRO reports to date confirmed governance arrangements operate effectively, several changes in structures and personnel necessitated a review of the Terms of Reference, overarching Data Custodian Model and associated operating practices. The review took place between May and December 2024, with the DGB approving revised Terms of Reference in October 2024.

12. The primary remit of the DGB remains unchanged, but Board responsibilities are now categorised as (a) Approach, (b) Deployment and (c) Assessment and Review. The revised Terms, attached as Annex A, are briefly summarised as follows, with Board agendas constructed to enable officers to meet these responsibilities:

    a. Approach
        - Achieve and maintain legislative, regulatory and corporate governance requirements
        - Ensure appropriate standards and policies are developed, in place and regularly monitored
        - Ensure data governance remains aligned to other corporate strategies, policies and plans, particularly the Digital and IT Strategy and key data principle.
    b. Deployment
        - Promote data governance and associated good practice across the Council and arms-length external organisations
        - Ensure all members of the DGB and DMT understand their roles and responsibilities, and are sufficiently trained to discharge such requirements
        - Monitor the provision and uptake of training provided to support effective data and information governance
    c. Assessment and Review
        - Receive and consider reports into breaches of confidentiality and security
        - Support the preparation of required reports, including but not limited to, the annual SIRO report, annual Data Protection report and scheduled Internal Audit reports
        - Review and update progress against identified audit and improvement actions
        - Schedule and undertake Data Quality and Information Governance risk assessments
        - Develop and examine performance measures that assess effectiveness and compliance
        - Review movement on the Data Maturity Curve, ensuring planned activity continues to move the Council towards the targeted 'advancing' stage.

13. These Terms of Reference will continue to be reviewed annually to ensure they facilitate ongoing legislative and regulatory compliance and enable the Board to effectively support the Council's business needs.

RISK MANAGEMENT AND ASSURANCE

14. The Council's Corporate Risk Register includes a risk in respect of Information Security and Information Governance. This risk is defined as "*There is a risk that Information; in whatever format; is not managed securely or that Information Governance across the Council and its ALEOs/partners is ineffective. This includes implementation of enhanced controls to meet the evolving working practices of the council such as the significant shift to home and hybrid working*".

15. The council identifies and monitors significant risk to its operations. The Information Security and Information Governance risk is assessed and monitored using the standard council-approved process for risk management. The inherent score of this risk is 25, having been assessed at the maximum score of 5 for both likelihood and impact.

16. The agreed approach to the management of key corporate risks sees all risks allocated to a member of CMT and a Corporate Working Group, with such responsible for assessing, monitoring, and reviewing in accordance with residual risk ratings. This particular risk is aligned to the Data Governance Board (DGB) with the Chief Officer (Business and Digital) presently identified as the Corporate Risk Lead.

17. The Corporate Risk Register (CRR) 2024-25 was approved by the Audit and Scrutiny Panel in August 2024, with the Panel considering the latest status of the CRR in October 2024. Both reports confirm that Information Governance and Information Security remains as a corporate risk given the impacts which breached, inaccurate or lost data could have on the Council achieving its priorities and stated objectives. Furthermore, in both reports, the Information Governance and Information Security Risk is evaluated as 'high' risk, carrying a residual risk assessment of 20 "*almost certain*" likelihood (5) and "*major*" impact (4). This risk was monitored regularly throughout calendar year 2024 but was not one of the corporate risks subject to formal reporting to the Corporate Management Team and Audit & Scrutiny Panel. As in previous years, formal reporting will be scheduled in accordance with the timelines identified by the Chief Officer (Audit and Risk).

18. The DGB most recently reviewed this corporate risk at its meeting of 4th December 2024, confirming the following security and governance controls remain in place to manage cyber and information risk.

Control (C) / Action (A)	***Description***
CON0000233	The framework of information governance policies supporting the council and the Digital and IT Strategy (i.e. Data Protection Policy, Payment Card Data Security Policy, Information Security Policy, Acceptable Use of IT Policy (and guidance), Records and Information Management Policy, and Records Management Plan) are well established in terms of ensuring the council has a suite of information governance policies to ensure that the council's approach to data is effective and compliant in relation to data governance and the arrangements required to ensure effective arrangements are in place for the safe and secure collection, storage, use, and sharing of data, including processes to safeguard personal data and support data quality.

Control (C) / Action (A)	*Description*
CON0000233	Governed by the Data Governance Board, all policies (except the Records Management Plan) are reviewed every two years. In respect of the Records Management Plan, the council is not the keeper of this, and the council are informed when they are required to update this. In the meantime, the council does undertake an interim internal review each year
ACT0001320	Review of the above, carried out on a biennial frequency, completed during 2023. Next reviews are on the DGB workplan and scheduled to be undertaken during 2025.
CON0001064	Secured Premises with secure storage and monitoring of security arrangements.
CON0001477	Corporate Records' Stores protected with CCTV, Disaster Recovery Plan, Fire Evacuation Plan, security checks during building closures, fire and intruder alarms, fire doors, shelving in accordance with BSI guidelines, pest monitoring, temperature and humidity monitoring, boxing of all records, archival enclosures for records, reduction of UV light.
CON0002051	A one council approach to data and information management is in place through the roadmap developed in September 2020.
ACT0001310	This risk is currently being enhanced in line with the Programme of Work to 2028 to better unlock the potential of data to support delivery of The Plan for North Lanarkshire by ensuring an accessible and single source approach to data that supports the organisation by providing insights and evidence that support decision making, planning, delivery, and continuous improvement as well as public reporting and transparency. This will incorporate all related aspects of data, including governance, quality, data maturity, spatial mapping, open data, and the supporting architecture and technology tools.
CON0002060	PROTECTIVE technical cyber security controls in place such as device authentication checks, multi-factor authentication, network segmentation, web gateways, email filtering solutions, etc.
ACT0001050	Conditional Access programme revised in December 2024, and approved by BMT, will be rolled out during 2025 as part of Windows 11 deployment.
CON0002061	DETECTIVE cyber security technical controls in place such as a security event and incident management, intrusion detection, and malware detection solutions, ongoing penetration testing, etc.
ACT00001051	Testing (by a non-Council organisation) of ICT security controls undertaken with findings reported to UK HMG Cabinet Office for independent evaluation.
CON0002062	RESPONSIVE cyber security technical controls in place inc. malware containment and recovery tooling.
ACT0000913	Arrangement entered with an experienced cyber incident response partner.
CON0002070	Register of Data Processing Agreements, Data Sharing Agreements and Data Protection Impact Assessments is in place. Improvements being undertaken through a corporate data protection review.

19. Over the course of 2024 further enhancements to the Council's information security governance and technical cyber security control suite were commenced and/or implemented. A programme commenced to create a structured suite of information security standards which will govern the Council's security posture moving forward. Email continues to be a source of unintended information leakage, and the Council has now procured product that aims to reduce the frequency of this occurring. Third-party cyber risk management is an increasingly important consideration for organisations of all sizes, and enhancements to existing processes are in flight which will improve the arrangements in place for assuring third parties in their use of Council data or connectivity to Council systems.

COMPLIANCE WITH DATA PROTECTION AND GDPR REQUIREMENTS

20. UK GDPR and the Data Protection Act 2018 categorise the Council as a Data Controller, with the DPO tasked with ensuring compliance with all associated data protection arrangements. Responsibilities include maintaining relevant policies, monitoring compliance with such, raising awareness of those policies and ensuring relevant training is provided to all staff to enable the Council to satisfy its legal obligations. Since May 2018, the Council has also had a legal obligation to undertake Data Protection Impact Assessments (DPIA) when processing personal data.

21. This section of the report highlights any breaches of confidentiality and security considered by the DGB between January and December 2024, alongside assessment of the remedial actions identified. Once considered and agreed, remedial actions are subsequently cascaded council wide through the Data Management Team (DMT).

22. Over and above the Data Protection Officer's annual report, the Chief Officer (Business and Digital Solutions) includes a summary of breaches and near misses within the service's six-monthly reporting to the Finance & Resources Committee. Details (up to July 2024) were most recently provided in September 2024.

23. For the reporting period in question (to November 2024), the Council recorded and investigated 102 data breaches, with 82 (80%) reported to Legal Services as required within 72 hours, and eight reported to the Information Commissioner's Office (ICO). Comparable figures for the 2023 calendar year are 109 breaches, with 61 (56%) reported within 72 hours, and two formally reported to the ICO. At first glance, the level of breaches is very similar, indicating good information management awareness and reporting. However, given breaches meeting the threshold for reporting to the ICO increased, there is concern that an increasing risk to the rights and freedoms of individuals could lead to personal information falling into the wrong hands.

24. Members are aware that information governance training has been an identified area of improvement activity over the last few years. Paragraphs 41 to 48 below demonstrate that the strengthened arrangements and increased oversight, monitoring and focus have led to significantly higher numbers of in scope employees competing their mandatory training, and so evidencing a greater understanding of requirements. Scope remains however to improve upon timely reporting of personal data breaches and 'near misses' to Legal Services within 72 hours of incidents occurring. The DPO has revised the breach reporting form, issued accompanying guidance, and established a new internal '24 hours' deadline to assist in improving ICO reporting compliance.

25. Chart 1 overleaf compares recorded breaches from January 2019 to December 2024. The high volumes recorded in August and December 2023, and June 2024 follow targeted action by services to complete employee mandatory training requirements, satisfying the previously approved improvement action.

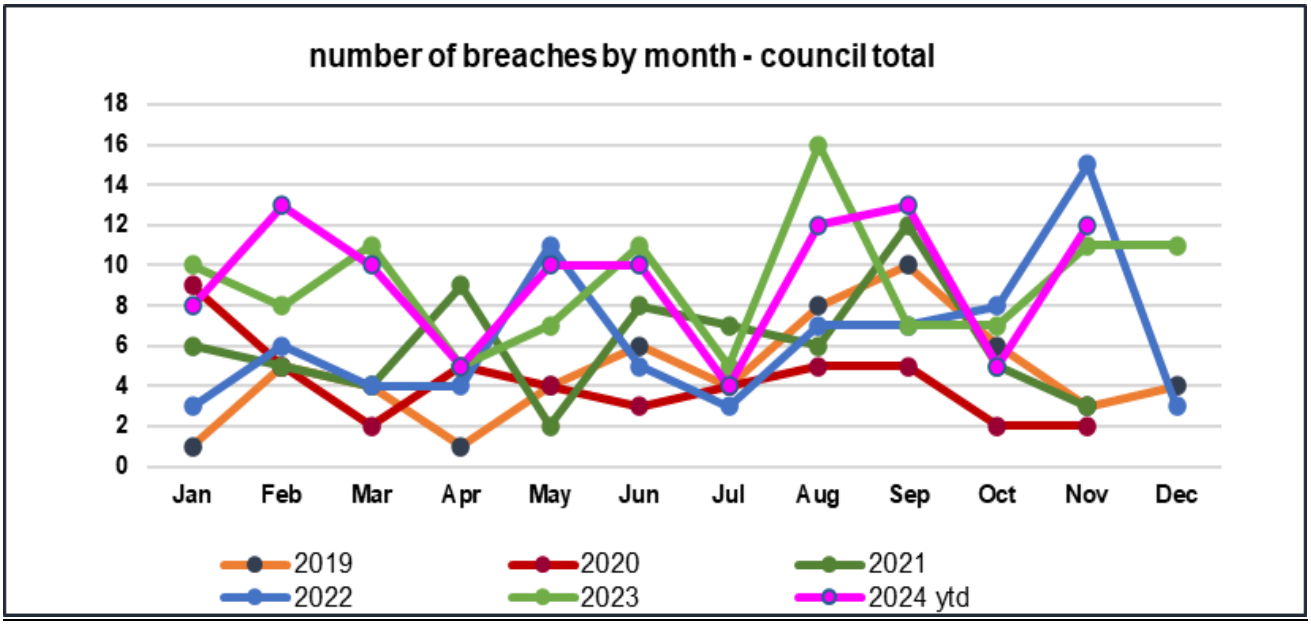


Chart 1

26. Chart 2 below, which analyses these details by service, indicates good correlation between completion of mandatory training and levels of reportable breaches. With services continuing to formally identify and report potential breaches, the Council has scope to act quickly to recover and/or prevent personal information from falling into the wrong hands.

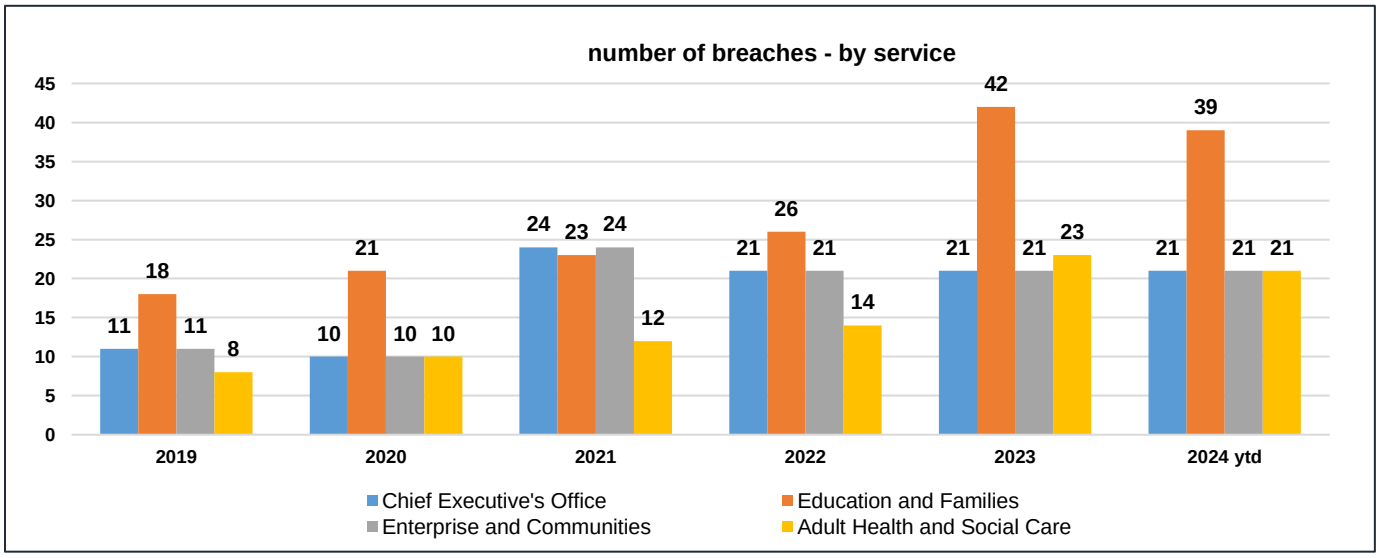


Chart 2

27. Categories of breaches include wrongful disclosure of data, device/documents left in insecure locations, unauthorised system/app use and failure to redact data. Per the DPO's Annual Data Protection reports, there was no enforcement action or fines applied by the ICO in respect of these breaches, but various recommendations were made. These are highlighted within Annex B, and include exercising caution with populated forms, ensuring information is fully removed from laptops being repurposed, reviewing the use of the scheduling assistant, and reviewing the security and procedures surrounding the issue of correspondence by services which include customer details. DGB discussions confirmed learning actions were appropriately documented, with all recommendations subsequently included within the action plans of both DGB and DMT.

ICT SECURITY AND CYBER RISKS

28. As the importance of digital information and networks grow, cyber security is of high importance and therefore a corporate priority. The type of risks posed include theft of sensitive corporate and personal data, theft or damage to data, threat of hacking for criminal or fraud purposes, and potential disruption to infrastructure such as Council ICT systems, intranet, and public facing website.

29. To highlight the scale of the cyber security threat, our firewalls trap and stop thousands of attempted network intrusions every week. In the month prior to writing, the Council's Corporate email security system identified 106,000 emails – 4% of the total sent to northlan.gov.uk addresses – as being sufficiently suspicious to warrant either delivery to the Council's Corporate email quarantine facility or prevented altogether at the email gateway. The Council's Corporate systems recorded 3.31M successful sign-ins. A further 319,000 attempted sign-ins failed, being a mix of apparent legitimate users plus others that were deemed sufficiently suspicious to be blocked. Of those that failed, 280,000 originated from the UK. It is worthy of note that 1,300 failed attempts alone originated from Russia. Publicised breaches over recent years (such as in respect of SEPA, British Library, Western Isles Council, Leicester City Council and Dumfries & Galloway Health Board) have individually and collectively demonstrated that public sector organisations can be significantly compromised following just one successful intrusion.

30. Strategically, the Council now faces risk on several fronts in terms of managing ICT security and cyber risks. These include:

    a. The ever evolving and growing cyber threat landscape. As noted in NCSC's Annual review 2024, "*Due to the changing geopolitical environment, including the ongoing war in Ukraine, the rise of state-aligned groups from around the globe, and an increase in aggressive cyber activity, it is highly likely the cyber threat to UK CNI [critical national infrastructure] has heightened in the last year.*" Even where public sector organisations do not find themselves directly compromised by successful cyber-attacks; it is becoming increasingly likely that their supply chain will be. Supply chain attacks can have serious consequences on the public sector. In June 2024, patient data managed by pathology testing organization, *Synnovis,* was stolen in a ransomware attack. Given the sensitivity of the data and the impact this breach had on the delivery of healthcare services, at the time it was described as "one of the most significant and harmful cyber-attacks ever in the UK." Organisations must spend ever greater effort and resource delivering activities capable of mitigating potentially catastrophic events, Growing appreciation of supply chain dependencies and the knowledge that internal processes can be severely compromised though cyber breaches affecting suppliers and vendors highlights the interconnected nature not just of IT systems but of wider business operations.
    b. Budgetary constraints affecting all public sector organisations in Scotland make it challenging to create and sustain vital posts to manage the Council's complex security domain effectively. Competition for suitably experienced and qualified security personnel across the marketplace is fierce, with such roles typically carrying premium reward expectations which exceed the Council's pay structure. This is called out explicitly in the Council's Workforce Plan where cyber security specialists are noted as being particularly difficult to recruit into public sector organisations like the Council. Succession planning is critical given there are high instances of 'single points of failure' within the Information Risk Management and Secure Access Teams; presently the loss

of a single staff member negatively impacts the scope and productivity of these critical council functions.

c. As digital technologies become more prevalent within the Council, so the cyber-attack surface increases. Providing the same level of protection as current over an increasingly broad and complex range of ICT services will become more challenging for the Council given projected budgetary pressures. This is particularly poignant given, across both the Education and Corporate estates technical staff are currently expected to support 550 servers, 12,173 desktop computers, 29,954 laptops, 13,979 tablet devices, 5,193 smart phones, circa. 260 server software/applications and over 3000 unique desktop/device types of software installations.
d. The continued rate of uptake of digital technologies to support service delivery means that ICT and cyber incidents will have an ever-increasing impact over time. If the Council loses staff to manage budget expectations, there will be a similarly increasing gap over time in the ability of the Council to 'fall back' on non-digital processes should a major ICT outage occur.
e. Artificial intelligence poses both a risk and an opportunity in terms of cyber security. It will enable threat actors to be more successful in their operations whilst providers of countermeasures will similarly take up the opportunities which AI offer.

31. To mitigate against cyber risks, the Council follows best practice wherever possible. We comply with the requirements of the Scottish Government Cyber Resilience Framework by currently having the Chief Officer (Business and Digital), as SIRO, identified as responsible for organisational cyber resilience arrangements. In addition, the Council works towards adoption of recommendations published by the National Cyber Security Centre (NCSC), who advise that cyber risk has been, and is likely to continue to, increase substantially. The Council follows published NCSC guidance and adopts the following approaches:

    a. **Compliance with the externally inspected Public Sector Network (PSN) accreditation via submission of the required IT health check findings, and implementation of recommendations identified as addressing potentially high-risk issues**. The Council recently achieved continued PSN compliance effective from 27th January. Certification remains valid for a further year, following acceptance by the Cabinet Office of the Council's plans to address 'high' vulnerabilities identified in respect of legacy applications such as HSMS, MySwis, eFinancials and CivicaOpenRevenues. Known vulnerabilities in respect of both financial products expect to be addressed through the Digital North Lanarkshire Programme of Work deliverable '*Review tools and products currently deployed to support the council's financial management arrangements, identifying and assessing options for longer-term suitability, as well as opportunities to deploy efficient and effective automation and self-service'*, which has a target completion date of March 2025.
    b. **Compliance with the Payment Card Industry Data Security Standard (PCI DSS),** with the Council continuing to be fully compliant across both person present and ecommerce payment channels and working towards achieving the same for the telephony channel as part of the procurement of a new unified communications platform.
    c. **A suite of malware protection products fully deployed** e.g., antivirus software, web filtering, and email malicious content/payload detection systems, together with real-time analysis of security threats identified and managed through deployment of Security Incident Event Management (SIEM) software. Responding to threats in a timely manner is supported through the actions of partner organisations and functions, such as the Scottish Government's Security Cyber Coordination Centre and subscribing to the services of a managed security operations centre.

d. **Firewalls installed to protect** the network, systems, and devices from external attack, exploitation, and data breaches, with an external contract in place to undertake penetrative testing, and any issues, anomalies or system vulnerabilities identified, investigated, and remediated.
e. **Operation of a robust "patching" regime**, with such automatically applied on scheduled dates where appropriate or as and when critical vulnerabilities are identified, and patches made available.
f. **Robust authentication and access control procedures** e.g.: multi-factor authentication in place to protect Council systems from unauthorised access and with continual improvements to access and authentication methods being made to address the threat landscape.
g. **ICT systems securely configured** as part of the initial commissioning process, with formal change control procedures being in place should system settings need to be modified.
h. Office "based" staff required to complete Mandatory Information Security Awareness training.
i. Non-office-based staff receive information security and governance awareness training through 'toolbox' delivered sessions.
j. Continued adoption of NCSC's active cyber defence toolkit as promoted through the Scottish Government's cyber security Public Sector Action Plan.

32. The Information Security and Information Governance risk process described in paragraphs 14 to 19 above does not record all activities underway to maintain the Council's security posture considering the threat landscape. Business and Digital officers routinely seek to improve arrangements by using Gartner's self-analysis and maturity assessment tools to direct future actions and confirm planned direction of travel. During the reporting period in question, the following ICT and cyber security focussed activities were undertaken to maintain a positive information governance assurance:

a. Resourcing within the Information Risk and Security Team was maintained at the increased level of 4.8 FTE. Recruitment is also under way for a temporary (funded for 2 years) Senior ICT Security Officer. It is planned to recruit a Graduate Developer into a security role at the start of 2025, and the creation of two posts as Security Operations analysts has commenced.
b. The Council has dropped use of the NCSC's 'Exercise-in-a-Box' evaluation tool to assess ICT resiliency capability. It is now coordinating with the Digital Office for Scottish Local Government to conduct a half-day workshop, scheduled for early 2025, with the aim of gaining a deeper understanding of the efficacy of Council effectiveness at responding to a major cyber security incident.
c. Operation of a phishing simulator solution to help train staff for the warning signs associated with one of the most prominent cyber threats facing organisations, phishing emails.
d. Management of third party cyber security risks, in particular supply chain risk, through focussed use of the Scottish Government's 'Cyber Security Procurement Support Toolkit.' Improvement actions under way are focusing on obtaining lifetime assurance of products and suppliers as appropriate, not simply at the procurement stage.
e. In recognition of the value of aligning with public sector peers, whilst fulfilling an action determined through a previous Information Security Maturity Assessment exercise, the Council is developing information security standards based on work already undertaken by the Department for Work and Pensions.

f. Activities are under way to better ensure that password usage meets NCSC's recommendations for length and structure, and marketing NCSC's 'three random words' approach to password creation, focusing on the Council's Education-based staff
g. Implementation of an automatically configured 'virtual private network' for all Council devices used remotely.
h. Continued awareness programme targeting all Council staff and employees, including focused sessions where appropriate. The set of mandatory training materials which all staff must review has been overhauled over the course of 2024 and will launch officially before the end of the 2024/15 financial year.

33. The Digital North Lanarkshire Programme of Work deliverable of '*ensure useful, secure, compliant and digital first applications are available to support critical but streamlined service delivery*' will transition all products to more secure and modern cloud-hosted solutions, but such cannot be achieved overnight. Prioritisation is therefore essential, and Business and Digital officers risk-assessed all critical legacy systems during 2023-24 to aid resource allocation. A summary of assessments is provided within Annex C.

34. As referenced in section 31(a) above, this deliverable is progressing with the priority business-critical – but ageing - systems (e.g. Housing Management System, Social Care System, Financial systems) which rely on older – and often unsupported – software and applications actively under consideration as follows:

    a. The Housing Committee awarded the contract for a replacement housing and asset management system to Civica UK Limited on 6th November 2024, with contract mobilisation and development of detailed implementation plans now underway.

    b. Deployment of Mosaic, the replacement case management system for MySwis, is well underway. Go-live is currently planned between March and May 2025, with such dependent on key functionality and integrations effectively meeting user testing requirements.

    c. The Financial Systems review is behind schedule. The Digital North Lanarkshire Programme Board considered progress against this deliverable at its December 2024 meeting. With limited progress evident to date, a target date for finalising options of March 2025, and a risk assessment of 20 (red) presented in respect of the current eFinancials product being used medium to longer-term, the Board agreed that lack of progress should be flagged to the CMT. The Board also instructed Financial Solutions to provide their project plan as a matter of urgency. The service has committed to doing so.

35. The council was not affected directly by any notable ICT or cyber security incidents during the 2024 calendar year. The potential consequences arising from supply chain compromises did not go unnoticed, however. Whilst the 'Crowdstrike' issue from June 2024 did not affect Council-managed systems, some managed services were impacted. Whilst outages were for a few hours at the most and did not affect critical functions, once again this highlighted the supplier dependent nature of business processes. The Council continues to be affected by day-to-day events that all organisations are affected by, and which are mitigated through the suite of technological and process controls in place, such as email filters, web gateways, network firewalls, web application firewalls, and anti-malware tools. The Council monitors centrally for issues that may affect its ICT service delivery through alerts provided by Scottish Government and the National Cyber Security Centre.

36. In summary, there continue to be successes in managing ICT and cyber risk, but challenges will grow given vital legacy systems – and the security vulnerabilities arising from them – cannot be addressed short-term. Vulnerabilities arising from legacy systems in use have previously hindered our ability to achieve an unqualified formal PSN accreditation. Whilst ongoing accreditation has recently been confirmed to January 2026, such is again based upon the Council taking action to address the high-risk vulnerabilities so identified.

CORPORATE GOVERNANCE ACTIVITY

37. The Council is committed to a clear strategy and sustainable framework for information governance and security so deploys its requirements through the Information Governance Policies contained within the approved Digital and IT Strategy. The 'Strategic Governance Framework – Annual Review and Refresh' report considered by the Audit and Scrutiny Panel in June 2024 confirmed these policies and the associated user guidance remain fit for purpose, having been allocated 'Green' RAG [1]status during this most recent evaluation.

38. Through the Data Governance Board (DGB) and Data Management Team (DMT) remits, the Council has identified Business Data Owners for its four key data classifications of customers, cases, people, and the organisation. Section eleven above illustrates however, that these are currently being reviewed following several changes to structures and key personnel. The DGB has continued to meet during the review period to ensure measures remain in place to maintain relevant compliance levels, and direct activities capable of moving the Council towards an 'advancing' (level 4) level of data maturity to (a) assist services in monitoring performance against The Plan for North Lanarkshire outcomes, and (b) view data as a 'single source of truth' to support strategic decision making, service delivery, cost reduction and risk management arrangements.

Data Maturity Assessment

39. Building upon improvement actions previously identified within the Council's Data and Information Management Strategic Roadmap, and activities underway to support the Council to achieve its targeted 'advancing' data maturity level, Business and Digital – aided by Gartner - re-assessed current levels of maturity in early 2024. The outcome indicates that corporate governance activity to date sees the council's overall Data Maturity Score improving from +1 (Initial/Basic) to -3 (Developing), against a benchmark score for similar organisations of 2+ (Basic).

40. Further details in respect of the Data Maturity Assessment are provided within Annex D, with Table 1 below summarising the key findings and actions which the DGB has built into its programme of work from 2024 onwards. A copy of this programme (as of December 2024) is provided as Annex E.

Theme	Functional Activity	NLC Score	Benchmark
Create the vision and strategy	Implement the strategy	4	2
Align data and analytics to Business Outcomes	Innovate the business model	2	2

[1] Green status – No requirement at this time to review or update this item, but such is planned for 2025.

Theme	Functional Activity	NLC Score	Benchmark
Develop the data and analytics organisation and talent	Develop data literacy	2	2
Create and maintain analytics content	Create and maintain semantic models	1	2
Integrate and manage data	Organise data assets	1	2
	Integrate data assets	1	3-
	Share data assets.	1	2
Govern data and analytics assets	Enforce governance policies	4	2
	Communicate governance policies	2	1+

Information Governance Training

41. The DGB and DMT have responsibility for continuously monitoring the actions required to manage information issues, risks, and cultural behaviour to improve existing data governance and management. Paragraph 12(b) above specifically references the importance of information governance training, an identified area of improvement and activity over the last few years.

42. At present, the majority of mandatory training modules need to be completed biennially, with the DGB regularly examining compliance levels; firstly, to gain assurances that staff are being trained in information governance; secondly, to identify areas requiring targeted activity, and finally, to assess the impact which planned improvements regarding performance monitoring have had

43. The 'SIRO Information Governance – Assurance and Performance Report (April 2022 to November 2023)' considered by the Finance and Resources Committee in February 2024 highlighted poor levels of mandatory training compliance council-wide, with an improvement action to 'raise the profile and prioritisation of Information Governance and Data Protection responsibilities' therefore identified.

44. Following consideration of the SIRO report, the Business Management Team (BMT) and Corporate Management Team (CMT) increased their oversight and monitoring to improve compliance levels across the council on *all mandatory training*, not solely information governance. This had led to strengthened arrangements being deployed, with Chief Officers now receiving monthly reports from the learning management system detailing staff within their business area who are either non-compliant with requirements or whose compliance with one or more of the mandatory modules is due to expire within the next month.

45. In revising arrangements, People Resources introduced the following RAG status for 'in-scope' employees below based on levels of non-compliance:

    a. RED – above 31% non-compliance
    b. AMBER – 21% to 30% non-compliance
    c. GREEN – 0% to 20% non-compliance

46. Table 2 below summarises non-compliance levels for the information management related modules as of 7th December 2024.

Mandatory Module	**Service Area – Non-Compliance %**			
	Chief Executives	Adult Health & Social Care	Enterprise & Communities	Education & Families
Data Protection Essentials	2%	16%	3%	11%
Information Security	2%	17%	4%	11%
Records & Information Management	3%	24%	4%	14%
Introduction to Risk	3%	21%	4%	13%
Data Protection Advanced	6%	20%	11%	16%

47. Illustrating that circa. 11,800 employees are considered in scope to complete information management mandatory training modules (except Data Protection Advanced – 1,869 in scope), chart 3 below presents the level and percentage of completions, per service, in December 2024.

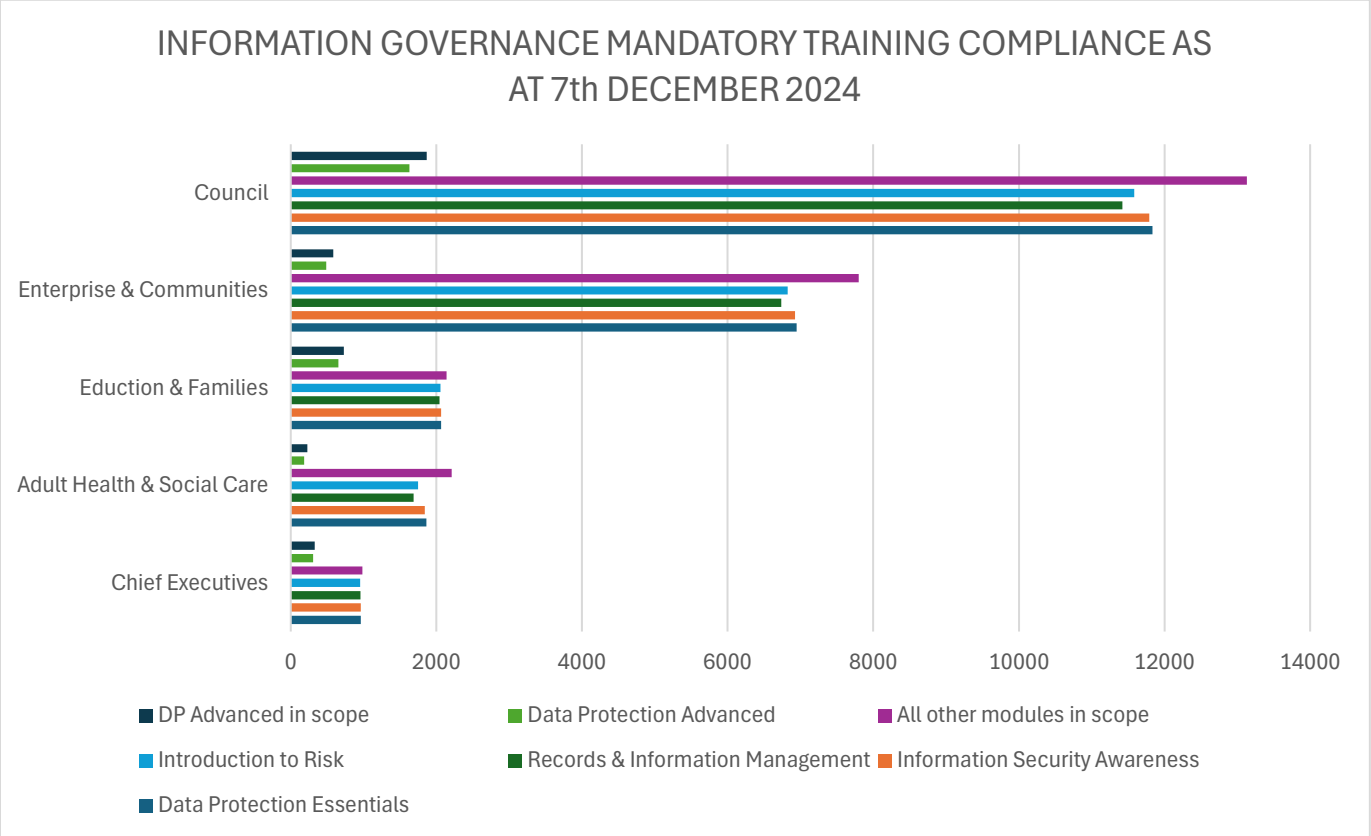


Chart 3

48. Finally, from a mandatory training perspective, chart 4 below tracks the peaks and troughs of training activity from January 2022 to December 2024, clearly demonstrating significant improvements in compliance levels following deployment of the strengthened monitoring and oversight arrangements.

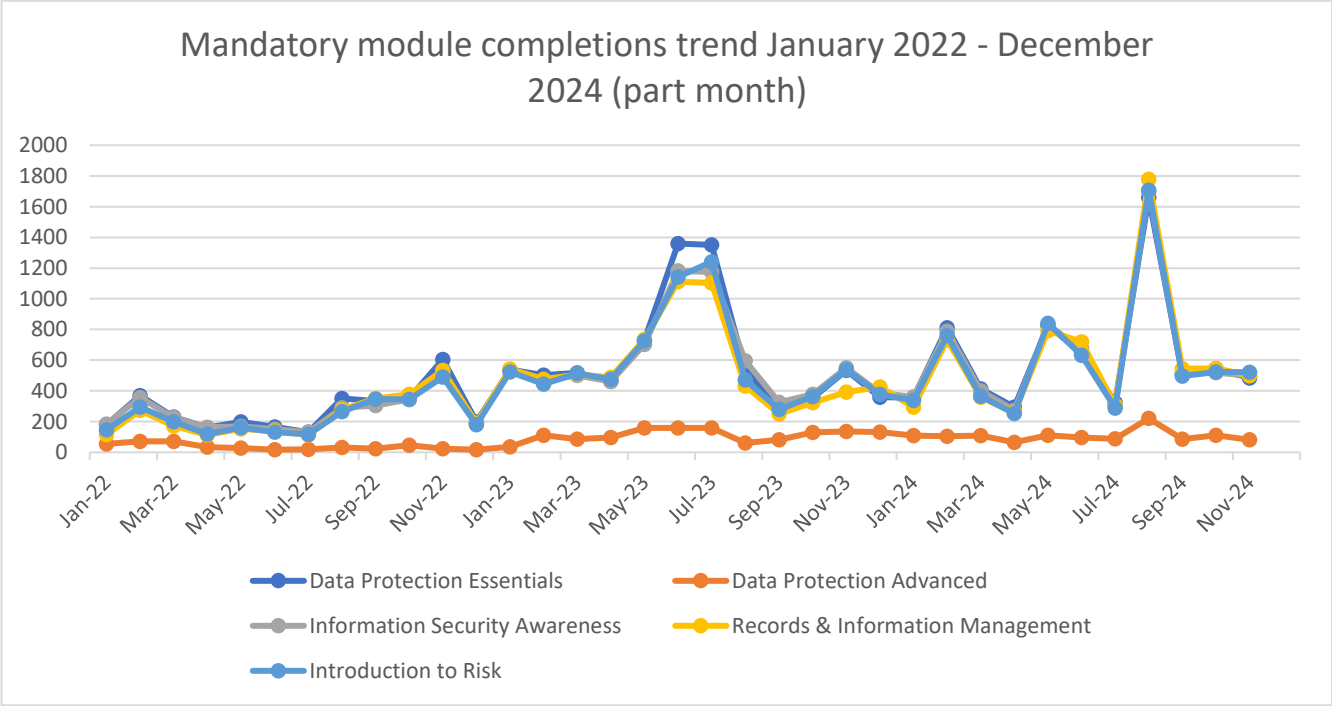


Chart 4

Records Management Plan

49. The Council has a Records Management Plan in place as required by the Public Records (Scotland) Act 2011 (PRSA). The plan outlines the Council's approach to Records Management and identifies key roles including the senior official responsible for records management, Data Protection Officer, operational Records Manager and Archivist.

50. The Records Management Team continues to work on the specific areas that the Keeper of the Records of Scotland has identified for improvement, namely Business Classification (File plan and Information Asset Register), Destruction Arrangements, Vital Records and Audit Trail. Following implementation of a file plan and physical records management using O365/Avepoint Opus, the DGB has undertaken to review the proposed approach to implementing semi-automated destruction in O365 and moving to roll this out in line with commitments made in the Records Management Plan in 2025/26.

51. The PRSA Assessment Team has a mechanism that allows authorities to self-report on its arrangements and commitments laid out in the Records Management Plan. The Council was commended for submitting a Progress Update Review (PUR) in 2022 and continuing to take its statutory obligations seriously. This report was published on the National Records of Scotland's website in November 2022. North Lanarkshire Council and North Lanarkshire Licensing Board Progress Update Review (PUR) Report by the PRSA Assessment Team 15th November 2022 (nrscotland.gov.uk). The Records Manager will submit a further PUR in 2025 and continues to liaise with the Assessment Team, informally, to ensure that any changes proposed in response to the ever-changing records management landscape will not conflict with the Council's responsibilities under the Act.

52. The Keeper of the Records of Scotland will in due course request a fully revised Records Management Plan to be submitted with accompanying evidence of progress made since the initial plan was approved in 2017. It is anticipated that the invitation will not be before 2026, with a six-month timeline available to complete and submit the new plan.

LIVE IMPROVEMENT PLAN

53. Paragraph 12 above highlights the DGB is responsible for directing required improvements in the Council's data governance arrangements. The detailed Terms of Reference, attached as Annex A below, and DGB workplan (Annex E) taken together illustrate how the DGB and DMT provide ongoing assurances regarding the Council's information governance. The workplan in particular outlines key tasks required, together with details of the responsible officers, and indicative scheduling.

54. By its nature, improvement activities and the workplan must be flexible and dynamic, with any new improvement areas identified by for example services, Business Data Owners, management, and Internal Audit appropriately incorporated. Having examined and assessed information governance activities throughout 2024, the SIRO has determined that further effort is required during 2025 in the following areas to strengthen the Council's information governance and data accuracy arrangements.

a. Raise the profile and prioritisation of Data Protection responsibilities

- Section 2 above illustrates everyone - staff and elected members - must understand the importance of information governance and security, as compliance with its requirements depends on all operating good practice.

- Whilst mandatory training completion and breach reporting rates were markedly improved during 2024, there is still concern regarding (i) the level of data breaches being reported to Legal Services within the 72-hour requirements, and (ii) levels of email misuse which led to potential data breaches. Further targeted promotion to be scheduled, ideally aligned with the launch of the refreshed information security mandatory training course, no later than the end of the 2024/25 financial year.

- Additional discretionary training, linked to refreshed requirements of Business Data Owners, Data Stewards, and Data Architects, to be developed and deployed during 2025

b. Refresh and strengthen approach to mitigating Cyber Security risks and vulnerabilities

- The Council continues to use PSN accreditation as the principle means of demonstrating external oversight of the Council's security posture, with compliance confirmed for one further year from 27th January 2025. Efforts are underway through the Digital North Lanarkshire PoW to reduce vulnerabilities associated with legacy ICT applications. Given outcomes will be closely monitored by the PSN assessors and UK Cabinet Office (PSN sponsor and accreditor), these areas of activity must be resourced as a priority.

- Paragraph 34(c) above illustrates Financial Solutions are committed to developing, and deploying, a project plan aligned to the PoW deliverable in respect of ensuring financial management systems used longer-term are '*useful, secure, compliant and digital first'.* The Digital North Lanarkshire Programme Board, Enterprise Architecture Governance Group (EAGG) and DGB should collectively ensure that oversight of this project, and its resourcing, is effective.

- Continue to develop and deploy the pipeline of information security standards in accordance with the 'production schedule' considered at the Digital North Lanarkshire Programme Board in December 2024.

- Enhance supply chain risk management by developing a proportionate framework to facilitate assurance of third-party products over the product lifecycle, agreeing monitoring mechanisms through the Digital North Lanarkshire Programme Board.

- Fully evaluate cyber security metrics presently being developed through the Digital North Lanarkshire Programme Board.

- In line with the programme of enhancements to conditional access controls approved at DGB and BMT in December 2024, allocate resources to ensure implementation is aligned with the deployment of Windows 11 compliant devices. Headline deliverables to include blocking legacy authentication; requiring Multi Factor Authentication (MFA) and deploying self-service password reset.

- Email continues to be the number one tool leveraged by malicious threat actors to breach Council cyber security controls. Considering this alongside data breaches linked to email misuse, the Council will roll out a technology solution during 2025 to enhance its email security, providing improved protection from incoming malicious emails and reducing the risk of users sending potentially sensitive emails to unintended recipients

c. Iterative deployment of the Data Governance Board approved Workplan (Annex E).

- The improvement actions identified in the DGB Self-evaluation exercise (2021) are now superseded by the DGB review of June 2024, and the DGB workplan attached at Annex E. This includes the following for example:

    - Enhancing the knowledge and understanding of all DGB members, especially those new to the role though the development of an induction pack for members, comprising role profile, FAQ, and jargon buster.

    - Reviewing the suite of performance measures that are in place to provide the DGB with the relevant assurances in respect of data governance to ensure these remain fit for purpose and in line with the DGBs updated terms of reference. This includes due consideration and implantation of more automatic data capture and reporting arrangements through PowerBI dashboards.

d. Enhanced implementation of the council's strategic approach to data and information management in line with the Programme of Work to 2028 and the DGBs updated Terms of Reference.

- To build upon the foundations established through the Data and Information Management Strategic Roadmap established in 2020, a range of inter-related activities are underway to ensure the councils use and approaches to data remain aligned and continue to ensure organisational compliance with the legislative and regulatory requirements relating to the handling and processing of information and provides assurance of ongoing improvements to manage information risks. This includes managing data in line with the CIPFA Delivering good governance in local government framework.

- Following completion of the DGB review in June 2024, the new working arrangements are in place and the next steps include a complete review of DMT, including Terms of Reference to ensure alignment with the updated DGB terms of reference and the refreshed approach to its operation.

- Implementation of a Data Hub as a single source for accessing corporate data that is a single source of truth for use across the council. This aims to unlock the potential of data and create meaningful insights that support the council in data management and information governance, as well as managing services and delivering the Programme of Work in line with The Plan for North Lanarkshire. This will incorporate all related aspects of data, including governance, quality, data maturity, spatial mapping, open data, and supporting architecture and technology (including continued development in the supporting tools, such as Power BI and Geographic Information System (GIS) to better automate processes and enhance data insights). Ensuring fit for purpose supports and approaches to building and cascading of skills across the council in terms of working with data and using the supporting tools will also be incorporated in line with corporate processes and requirements.

CONCLUSION

55. In summary, significant progress to strengthen the Council's approach to managing its information risks continued over the period of this report with sections 20 to 52 above providing relevant context and detail.

56. Improvements can always be made, and with a residual risk score of 20 prevalent in respect of our Information Governance and Information Security corporate risk (October 2024), this subject matter remains a high priority improvement area for the Council.

57. A detailed improvement plan exists and is monitored by the DGB. A summary of the priority actions at December 2024, is detailed in section 54 above. Progress against these will be managed by the DGB from January 2025 onwards, who will look to further develop policies, guidance, standards, processes, and approaches as appropriate to improve awareness, understanding and compliance with legislative requirements and good practice.

58. With our PSN accreditation dependent upon UK HMG Cabinet Office being satisfied we have sufficient protections in place to address high-risk vulnerabilities in our ageing critical systems, and people and financial resources projected to remain extremely scarce and challenging, there is heightened concern in these times of increasing cyber-attacks regarding the Council's ability to fully secure the data held within older legacy business applications. Actions are identified and largely underway through the approved Programme of Work and capital investment programme to address this growing risk, but concern remains regarding the organisation's capacity to resource required activities in a timely manner.

Katrina Hassell
Chief Officer (Business and Digital)

Data Governance Board
Terms of Reference

A. Purpose

The purpose of the Data Governance Board is to maintain strategic oversight and implementation of the council's approach in relation to data governance and to secure the relevant assurances that effective arrangements are in place for the safe and secure collection, storage, use, and sharing of data, including processes to safeguard personal data and support data quality. This includes responsibility for developing and overseeing the implementation of strategies, policies, procedures, and standards in relation to data governance and data management, and for directing improvements in accordance with legislative, regulatory and corporate governance requirements and in support of the organisation's corporate vision and strategy. The Data Governance Board is also responsible for directing and overseeing the work of the Data Management Team and ensuring measures are in place to monitor compliance across the council and its arm's length external organisations.

B. Legislative, regulatory, and corporate governance requirements

- Data Protection Act 2018.
- Freedom of Information (Scotland) Act 2002.
- Public Records (Scotland) Act 2011.
- CIPFA Good Governance in Local Government Framework (2016) in respect of Managing Data.

C. Membership

Core members *consistent attendance*

- Chief Officer (Business and Digital) - Chair
- Chief Officer (Legal and Democratic) - Vice-Chair.
- Business Strategy Manager.
- Technology Strategy Manager.
- Corporate Records Manager.
- Strategy and Performance Manager.
- Nominated representatives from services aligned to data roles and responsibilities in respect of the data entities for cases, customers, organisation, place, and people.
- Officer who holds the role of the council's Data Protection Officer (if not one of the above).
- Officer who holds the role of the council's Senior Information Risk Owner (SIRO) (if not one of the above).
- Chair of the Data Management Team.
- Management Support Officer - minutes.

Given the specialist data governance knowledge that is required to understand the work of the Data Governance Board, substitute members are only permitted in exceptional circumstances. This is critical to ensure those attending meetings have the appropriate knowledge, skills, and abilities to discharge their duties and that this is enhanced over time through ongoing and consistent involvement in the Board's business.

Non-core members *attendance as required depending on the business to be dealt with*

- Subject matter experts.

D. Remit

The primary remit of the Data Governance Board is noted below against three categories of Board responsibilities (approach, deployment, and assessment and review):

Approach

1. To be assured that the council achieves and maintains compliance with legislative, regulatory, and corporate governance requirements, including that listed in section B.

2. To ensure the council has effective data governance standards and policies in place which have been developed in line with legislative, regulatory, and corporate governance requirements as well as accompanying policies, guidance, and professional codes of practice.

3. To maintain oversight of the council's data governance policies and standards to ensure they remain effective, up to date, and fit for purpose, including (but not limited to) the Data Protection Policy, Information Security Policy, Records and Information Management Policy, Payment Card Data Security

Policy, Acceptable Use of ICT Policy, Records Management Plan, and in respect of Data (i.e. governance, quality, and open data).

4. To ensure the council's approach to data governance is aligned to, and effectively supports, what the organisation ultimately aims to achieve through its corporate strategy, i.e. through The Plan for North Lanarkshire and the delivery vehicle of the Programme of Work.

5. To ensure the council's approach to data governance aligns to other corporate strategies, policies, and plans as appropriate. This includes, but is not limited to, the Digital and IT Strategy and its data principles:
   a) Data is an asset - Data is an asset that has value to the council and other parties and must be managed accordingly.
   b) Data has an owner - data will have a named Information Asset Owner accountable for the data quality and currency.
   c) Common data definitions - Data is defined consistently throughout the council, standardised, understandable, and distributed.
   d) Information security - Data is protected from unauthorised use, disclosure, and change.

Deployment

6. To ensure the council's data governance standards, policies, and procedures:
   a) Enable the organisation and staff to discharge their duties regarding the use of information.
   b) Ensure that personal data held by the council is accurate, kept confidential and secure, accessed only by those with legitimate need, and available when required.
   c) Make sure records (paper and electronic) are disposed of in an appropriate manner, relative to their confidentiality when no longer required and in line with records management policies and codes of practice.

7. To promote data governance and associated good practice across the organisation and its arms-length external organisations. This includes communicating the importance of data governance to all staff, promoting a council wide culture that data governance is the responsibility of everyone, advocating for data governance initiatives, fostering a data driven culture within the organisation, and developing (and contributing to) regular reports, newsletters, website content, and other publicity materials.

8. To maintain oversight of roles and responsibilities related to data governance, such as data owners, data stewards, data custodians, data admin, and data users. This includes ensuring roles are clearly defined and that individuals in these roles have appropriate training and guidance to perform their duties effectively.

9. To monitor the provision and uptake of training provided to support effective data and information governance across the council in order to ensure that staff are trained, comply with, and understand the consequences of not adhering to relevant policies and procedures.

10. To set the Terms of Reference for the Data Management Team and oversee and direct its work in cascading and co-ordinating the implementation and deployment of all relevant data governance strategies, policies, plans, standards, and arrangements as approved by the Data Governance Board.

11. To ensure all members of the Data Governance Board and Data Management Team are provided with appropriate training and guidance in order to discharge their duties as members of the respective group.

Assessment and review

12. To receive and consider reports into breaches of confidentiality and security and where appropriate undertake or recommend remedial action. This includes promoting learning that arises out of investigations into data breaches.

13. To receive, review, contribute to, and sign off (where required) reports in advance of further oversight or scrutiny by the Business Management Team / Corporate Management Team or one of the council's Committees. This includes:
   a) Assisting the Senior Information Risk Owner (SIRO) in the preparation of the annual Information Governance Annual Report and signing this off prior to submission in line with the relevant

timescales.

b) Reviewing the annual Data Protection report produced by the corporate Data Protection Officer.
c) Scheduled Internal Audit reports pertaining to data or information governance.
d) Reviewing and updating progress against identified audit actions and responding to new audit recommendations as required.

14. To regularly review the Board's data governance programme and one council approach to assess its effectiveness, identify areas for improvement, and makes necessary changes to the respective data governance arrangements, policies, and procedures. This review includes ensuring the council:
    a) Undertakes - or commissions - annual assessments and/or audits of its data governance policies, procedures, and arrangements.
    b) Carries out a regular data quality assessment.
    c) Regularly reviews its movement on the data maturity curve, ensuring that planned activity is directed towards achievement of the advancing stage of the maturity scale.
    d) Has appropriate data governance performance measures in place to assess effectiveness and compliance, with regularly monitoring and reporting processes in place to ensure Board oversight and inform continuous improvement where required.

15. To maintain regular oversight of risks on the Corporate Risk Register in relation to information governance and security to ensure the supporting controls and actions remain relevant and in place to mitigate against the risks identified.

E. Decision making

The Data Governance Board is the council's main decision-making body in respect of strategic data governance issues.

The Data Governance Board is accountable to the Business Management Team (in respect of the council's compliance with legislative, regulatory, or corporate governance requirements) and the Corporate Management Team (in respect of deployment and compliance across services) and will, where required, escalate matters as appropriate for corporate decision making, endorsement, or action.

F. Governance and accountability

Through the Chair, the Data Governance Board will ensure reports are provided to the Business Management Team or Corporate Management Team, as appropriate, where matters have an impact as per the respective responsibilities as noted in section E.

Where matters fall within the scope of the Scheme of Administration, reports will be submitted to the Audit and Scrutiny Panel through the Chair.

The Terms of Reference for the Data Governance Board shall be reviewed at least annually to ensure the Board continues to meet the business needs of the council and ensure ongoing compliance with legislative, regulatory, and corporate governance requirements.

G. Operation

The Data Governance Board has been constituted at the request of the Corporate Management Team.

Meetings will be held on a bi-monthly basis. The Chair may convene a meeting at any time to consider matters of an urgent nature.

The agenda and any working papers will be circulated five working days working week before meetings. Minutes will be published on the Data Governance Microsoft Teams site and the link circulated to members of the group and other individuals, or groups as required.

Annex B

Information Commissioner Office Guidance
North Lanarkshire reported data breaches

The ICO issued the following guidance to the Council regarding its reported breaches:

- The importance of accurately recording information about data subjects within records and ensuring that any manually recorded information is accurately migrated into any electronic record;
- Any attachments to emails should be correctly identified and that any manual correspondence be accurately addressed and contain only information properly intended for that recipient;
- Populated forms should not be provided in response to requests for blank forms;
- Forms populated with an individual's personal data must not be used as a template;
- Appropriate double checking and verification measures should be in place;
- Managers must remind staff of their responsibilities to ensure that personal data is processed securely.
- In relation to cleansing of laptops, there must be appropriate checks to ensure that any personal information is removed before issuing these laptops for use in school classrooms;
- Conduct appropriate checks of any devices that are used by pupils to ensure that there is no personal information saved on them in error;
- Changes of procedures should be communicated to all staff with routine testing of the effectiveness of measures in place, and appropriate checks that staff are adhering to these measures;
- Remind staff of the provisions of section 170 of the Data Protection Act 2018 which states that it is a criminal offence to unlawfully obtain, disclose, or retain personal data without the consent of the controller;
- Consider use of the schedule assistant to allow further time to check contents and recipients are correct;
- Documents containing personal data should be password protected before they are sent electronically, with the password sent in a separate email;
- Only members of staff who are required to use the personal data should have access to it;
- Care should be taken when discussing personal data in the presence of anyone who isn't authorised to know about it;
- When individuals request that their personal data is handled in a particular way for example, where there are concerns about their personal safety then this should be clearly marked on their file and vigilance should be taken to ensure that these requests are complied with;
- Ensure systems are up to date and correct.

Annex C

Risk Assessment Summary

Table of Risk Scores of P1 Applications over Time

Application/ System	Current (Dec 2023) Residual Risk Level	Future Forecast – 1yr (Dec 2024)	Future Forecast – 3yr (Dec 2026)	Future Forecast – 5yr (Dec 2028)
Housing Services Management System	8	12	20	25
Building and Cleaning Management System	6	9	16	20
giFT (Unix file transfer system)	6	6	12	16
Confirm*	4	2	N/A	N/A
Common Housing Register /Mutual Exchange	6	6	9	12
Home Insurance*	2	2	N/A	N/A
eFinancials	8	12	20	20
Open Revenues	12	12	16	20
ASH Debtors	3	3	3	3

- Risk was assessed using the Council's 5x5 risk scoring matrix.
- Lowest risk score achievable is 5, highest 25.
- **All scores are residual, based on future forecasts of supportability of product.**
- **High risk scores indicate increased likelihood of product becoming more costly to support and maintain operationally.**
- * Indicates where a system is intended to be transferred to a managed Cloud-hosted platform or deprovisioned

Observed Risk Factors by Application

Application/System	Observed Risk Factors
Housing Services Management System	➢ No 3rd party supplier support contract ➢ Bespoke progress-based application, developed in-house to the council ➢ 2 x contracted developer staff: aging demographic is a factor ➢ No release lifecycles. ➢ Vulnerabilities are likely to arise in the supporting operating systems and software languages will need to be patched
Building and Cleaning Management System	➢ On premise server hardware is already 6-7 years old and out with warranty. ➢ BCMS is another bespoke in-house product. ➢ No 3rd party support and relies on small support team focusing on minor adaptations and issues. With a single technical support person remaining. ➢ Many systems that were once part of BCMS have now moved to other SaaS offerings e.g. HR records management, payroll
giFT (Unix file transfer system)	➢ giFT is a computer software daemon, which runs as a background process.

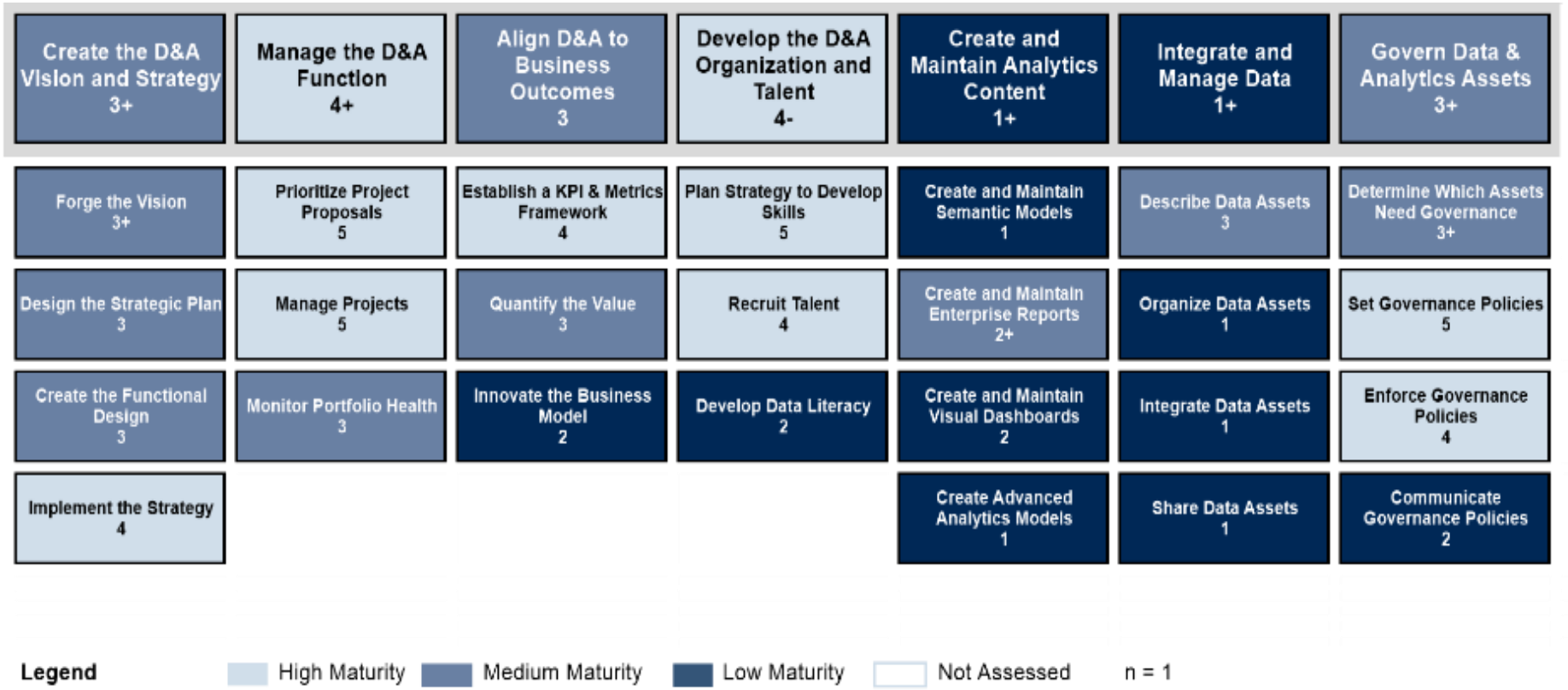
Annex C

Risk Assessment Summary

Application/System	Observed Risk Factors
	➢ Council developed gift into standalone application for file transfers ➢ Been maintained for 20 years but developers reduced with a single developer remaining. ➢ No 3rd party support contract
Confirm*	➢ Off the shelf product ➢ Support contract ➢ Regular updates ➢ Confirm was mid-transition to software as a service mid-evaluation, and fully migrated in June 2024.
Common Housing Register /Mutual Exchange	➢ CHR is a bespoke solution developed 2008/2009 ➢ Closely linked to HSMS ➢ CHR is a bespoke in-house product. With no 3rd party support and relies on 2 contracted developers' availability. ➢ Aging demographic is a factor.
Home Insurance*	➢ Bespoke in-house developed by North Lanarkshire Council in 1995 ➢ Originally supporting 10,000 customers ➢ Customers have decreased through cheaper offerings or moving house and selling up. ➢ Service and product have now been closed down.
eFinancials	➢ eFinancials relies on underlying UNIX platform, with high reliance on Java plugins which are difficult to support and have previously been linked to breaches in other organisations ➢ Areas of the infrastructure will be end of life within the next 4 years. This reflects on the increased risk scoring for the 3rd and 5th years ➢ Current plans for upgrades of Windows OS have not been considered within this risk assessment as these are handled by the End user computing team and organisation wide ➢ Hardware supporting some of the Operating Systems will have aged and may require replacement to support future OS
Open Revenues	➢ Current database software is out of support ➢ Lack of regular software updates from supplier ➢ Current Java software is out of date & problematic to support ➢ Lack of well-proven DR capability for system ➢ Risk of cyber breach is high due to lack of software updates & regular security reviews
ASH Debtors	➢ System is hosted in a preferred environment, NLC's Azure cloud ➢ Application on most recent version ➢ No current operational support or compliance issues

Data Maturity Assessment

How mature are our data and analytics functional activities?



Maturity: Measured on a scale ranging from 1 (Low) to 5 (High), maturity measures how advanced an organization's development is in a functional activity relative to Gartner's best practice research. Maturity scores are refined with a (+) or (-) to indicate intermediate levels of maturity.

Data Governance Board
Roadmap and Workplan (as of December 2024)

The agenda will be structured around items which are categorised in relation to the type of assurance they provide to the Data Governance Board to enable the Board to fulfil its requirements as per the Terms of Reference and be assured that the council's data governance arrangements are robust. The following programme of work sets out the Board's recurring agenda items in this respect.

All other proposed agenda items (and specific projects / actions) will be subject to a triage process that is undertaken in line with the Terms of Reference for the Board so that the Board is allowed due consideration of the piece of work at the appropriate moment during its lifecycle.

This programme will be reviewed prior to each meeting and updated in line with the minute and action note from each meeting, anything added to the programme will be noted on the action note accordingly.

Agenda items	Responsibility for brining agenda item to Board	9 October 2024	4 December 2024	29 January 2025	26 March 2025	21 May 2025	16 July 2025	10 September 2025	5 November 2025	Board purpose
1. *Policy review and approve:* • Annual review of Data Governance Board terms of reference.	Katrina Hassell	**X**						**X**		Approach / Deployment / Assessment and Review
2. *Policy review and approve:* • Update to the Data Protection Policy (v 7.0 June 2023).	Archie Aitken				**X**					Approach
3. *Policy review and approve:* • Update to the Information Security Policy (v4.0 June 2023).	Rob Leitch				**X**					Approach
4. *Policy review and approve:* • Update to the Records and Information Management Policy (v 5.0 June 2023).	Fiona Hughes				**X**					Approach
5. *Policy review and approve:* • Update to the Payment Card Industry Data Security Policy (v1.0 June 2023).	Rob Leitch				**X**					Approach
6. *Policy review and approve:* • Update to the Acceptable Use of ICT Policy (v4.0 November 2023).	Rob Leitch								**X**	Approach
7. *Performance review and identification of actions for the Board reps and/or actions to be cascaded to the Data Management Team to implement:* • Data Protection annual report.	Archie Aitken						**X**			Assessment and Review

Data Governance Board

Roadmap and Workplan (as of December 2024)

Agenda items	Responsibility for brining agenda item to Board	9 October 2024	4 December 2024	29 January 2025	26 March 2025	21 May 2025	16 July 2025	10 September 2025	5 November 2025	Board purpose
8. *Performance review and identification of actions for the Board reps and/or actions to be cascaded to the Data Management Team to implement:* • Senior Information Risk Owner (SIRO) annual report.	Katrina Hassell		X	X						Assessment and Review
9. *Performance review and identification of actions for the Board reps and/or actions to be cascaded to the Data Management Team to implement:* • Mandatory e-learning statistics.	Gillian Quinn		X		X		X		X	Assessment and Review
10. *Performance review and identification of actions for the Board reps and/or actions to be cascaded to the Data Management Team to implement:* • Performance indicators.	Susan Lawrie			X		X		X		Assessment and Review
11. *Risk management review:* • Following quarterly review and deep dive update in respect of the corporate risk for Information Governance and Information Security.	Rob Leitch		X	X	X	X	X	X	X	Assessment and Review
12. *Deep dive:* • Into the roles and responsibilities of reps on the Data Governance Board (and Data Management Team), including the purpose and operation of the Data Custodian Model in practice.	Susan Lawrie	X	X	X						Approach and deployment
13. *Deep dive:* • Into the role and purpose of the Data Management Team.	Katrina Hassell			X						Approach / Deployment / Assessment and Review
14. *Deep dive:* • Into the data maturity assessment.	Susan Lawrie				X					Approach / Deployment / Assessment and Review

Data Governance Board

Roadmap and Workplan (as of December 2024)

Agenda items	Responsibility for brining agenda item to Board	9 October 2024	4 December 2024	29 January 2025	26 March 2025	21 May 2025	16 July 2025	10 September 2025	5 November 2025	Board purpose
15. *Communication:* • Ongoing action - where required - in relation to agreement of items which require to be: (a) Escalated to the Corporate Management Team / Senior Management Team or other Board/Group. (b) Cascaded to the Data Management Team for (i) implementation, (ii) to provide a report / update back to a future DGB meeting, (iii) for information. (iii) Communicated wider across the organisation.	Katrina Hassell	X	X	X	X	X	X	X	X	Approach / Deployment / Assessment and Review
16. *Accreditations:* • Public Services Network compliance.	Rob Leitch				X					Assessment and Review
17. *Annual review:* • Data sharing agreements.	Archie Aitken					X				Assessment and Review
18. *Business added to programme from DGB meeting Action Notes:* a. From DGB meeting on 19/06/24 - Retention schedule to be a regular agenda item to ensure it remains current and to ensure compliance and consistency throughout services (in line with the Records and Information Management Policy).	Fiona Hughes	X			X			X		Approach / Deployment / Assessment and Review
b. From DGB meeting on 19/06/24 - Open data report to be brought back to the DGB.	Linda Johnston							X		Approach / Deployment / Assessment and Review
c. From DGB meeting on 14/08/24 - DGB information pack and glossary to be created.	Katrina Hassell / Susan Lawrie			X						Approach / Deployment / Assessment and Review
d. From DGB meeting on 09/10/24 - Work to be undertaken to determine the programme of communication which requires to	Fiona Hughes			X						Approach / Deployment / Assessment and Review

Data Governance Board

Roadmap and Workplan (as of December 2024)

Agenda items	Responsibility for brining agenda item to Board	9 October 2024	4 December 2024	29 January 2025	26 March 2025	21 May 2025	16 July 2025	10 September 2025	5 November 2025	Board purpose
be circulated to employees regarding the use and adherence to the data retention schedule.										
e. From DGB meeting on 04/12/24 - Regular updates from the Lanarkshire Data Sharing Partnership Board to the DGB to be a regular item on the agenda.	Graeme Cowan		X		X		X		X	Approach / Deployment / Assessment and Review
f. From DGB meeting 04/12/24 - Demo to come back to the DGB in January 2025 regarding the electronic records management system to see this in practice and determine the next steps.	Fiona Hughes / Tracey Hughes			X						Approach
g. From DGB meeting 04/12/24 - Update to come back to the DGB in January 2025 regarding the master data management system.	William Cunningham			X						Approach