North Lanarkshire Council
Report

Audit and Scrutiny Panel

☐ approval ☒ noting **Ref** KH **Date** 09/12/21

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

From Katrina Hassell, Head of Business Solutions

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

Executive Summary

In response to the Information Commissioner's Office (ICO) audit of our data protection, security, and governance arrangements in 2012, the former Executive Director of Finance & Customer Services was appointed to the role of Senior Information Risk Owner (SIRO), with two overview reports regarding information governance effectiveness subsequently considered by the Corporate Management Team during 2014 and 2015.

Following several Council restructures, SIRO responsibilities transferred to the former Head of Revenue & Efficient Government Services, with such now resting with the Head of Business Solutions. Required to be a member of the Senior Executive team (CMT), the SIRO has ownership of the Council's information risk policy, and acts at the strategic level as the advocate of information assurance and risk.

In June 2019, Internal Audit issued findings in respect of the adequacy and effectiveness of the Council's approach to information governance issues, with such assessed as "reasonable assurance". However, a key recommendation from that report was the requirement to present an annual overview report to senior management and elected members of the Council's information governance arrangements, performance and compliance against key expectations and requirements.

This report aims to satisfy that requirement with details for financial years 2019-20 and 2020-21 presented for Panel consideration. The Head of Business Solutions will revert to the recommended annual report from financial year 2021-22 onwards, with such always reflective of any live Internal Audit recommendations.

This SIRO report aims to provide assurances that information risks are being effectively managed. It details the improvement actions which the Data Management Team (DMT) have planned to further improve awareness and understanding, to ultimately ensure the Council can comply with legislative requirements and good practice.

Recommendations

It is recommended the Audit and Scrutiny Panel:

(1) Note the activities which have been undertaken or are underway to enable the SIRO to provide assurances information risks are being effectively managed; and
(2) Note the activities and next steps planned to further improve the Council's information governance arrangements.

The Plan for North Lanarkshire

Priority	All priorities
Ambition statements	All ambition statements

1. Background

1.1 This report provides an update relating to the responsibilities of North Lanarkshire Council's Senior Information Risk Owner (SIRO) and outlines activity and performance related to information governance. It provides assurances that information risks are being effectively managed; what is going well, and where improvements can be made

1.2 The detailed report contained within Appendix 1 covers financial years 2019-20 and 2020-21, with details in respect of the 2019-20 year delayed facilitating an assessment of any additional requirements arising from deploying the new technologies envisaged within the Council's DigitalNL transformation programme.

---

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. SIRO responsibilities transferred to the Head of Business Solutions in September 2019. As SIRO, the Head of Business Solutions took action to address Internal Audit recommendations (June 2019) in respect of information governance, with such including a requirement to present an annual overview report to senior management and elected members of the Council's information governance arrangements, performance, and compliance.

2.3. Significant effort has been directed towards formalising and improving information governance management arrangements, with such detailed within sections 48 to 72 of the detailed SIRO report provided as Appendix 1. Key highlights for Panel consideration include:

- Corporate Governance arrangements refreshed (December 2019), with a Data Governance Board (DGB) and Data Management Team (DMT) established to develop, implement, and ensure compliance with data governance and management strategies, policies and standards;
- Corporate recording system for Subject Access Requests implemented (December 2019);
- Mandatory Data protection essentials training revised and launched (February 2020);
- Information Security and Information Governance corporate risk workshop (February 2020) detailed current roles and responsibilities of DGB and DMT members;
- Fully refreshed Information Governance Policy Framework approved by the Policy & Strategy Committee in June 2021;

- Mandatory data protection and information security training modules revised and launched (July 2020);
- Data and Information Management Strategic Roadmap approved by the Transformation and Digitisation Committee (February 2021);
- Information Governance KPIs established and approved by DGB (October 2020);
- Focus of DGB further revised to facilitate change from service based to functional representation, with membership now aligned with master data entities of Customer, Cases, Employees and Place (December 2020).

2.4. Complementing the Corporate Data Protection Officer's annual reports to the Finance and Resources Committee, sections 20 to 47 of the SIRO report detail compliance with prevailing legislative and regulatory requirements. Incidents requiring investigation and areas identified for further improvement are also highlighted for Panel consideration.

2.5. Sections 48 to 53 focus specifically on ICT Security and Cyber risks and advise the Panel of the accreditations and approaches adopted by the Council to mitigate against this high-risk area.

2.6. Paragraphs 54 to 56 detail actions taken to ensure compliance with the Public Records (Scotland) Act 2011

Next steps

2.7. 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 financial years 2019-20 and 2020-21, the live improvement plan detailed in section 74 of the Appendix highlights activity planned at March 2021 to strengthen existing arrangements.

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

a. Raising the profile and prioritisation of Information Governance and Data Protection requirements;
b. Refreshing our existing approach to mitigating Cyber Security risks;
c. Mapping Mandatory and Discretionary Training to Roles; and
d. Incremental implementation of the Data and IM Strategic Roadmap (the Roadmap)

2.9 Improvements can always be made to our information governance arrangements, and with a residual risk score of 20 (March 2021) 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. Equality and Diversity

3.1. **Fairer Scotland Duty**
There is no requirement to carry out a Fairer Scotland Duty assessment on this report; no new strategic decisions are being made.

3.2. **Equality Impact Assessment**

There is no requirement to carry out an equality impact assessment on this report.

4. Implications

4.1. **Financial impact**

There are no 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, section 51 of the SIRO report so appended illustrates we must also consider costs involved in achieving compliance with good practice standards, as such can be cost prohibitive for the Council to achieve given its complex portfolio.

4.2. **HR/Policy/Legislative impact**

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.

4.3. **Technology/Digital Impact**

Sections 48 to 53 of the SIRO report focus specifically on ICT Security and Cyber risks. The council operates a complex technology network, and through its DigitalNL programme, is looking to significantly change its server, applications, and software estate, as well as the underlying connectivity. All changes will be considered by the appropriate corporate working group.

4.4. **Environmental impact**

There are no implications arising from this report.

4.5. **Communication Impact**

Section 74 of the SIRO report highlights everyone – staff and elected members – must understand the importance of information governance and security, which when combined with lower than desired mandatory training take-up does illustrate a requirement for ongoing communication of requirements.

4.6. **Risk impact**

4.6.1. 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 Head of Business Solutions 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.

4.6.2. Improving our information governance arrangements will positively impact the Council's risk management arrangements, consequently leading to greater confidence in the accuracy of data used to support decision-making.

5. Measures of success

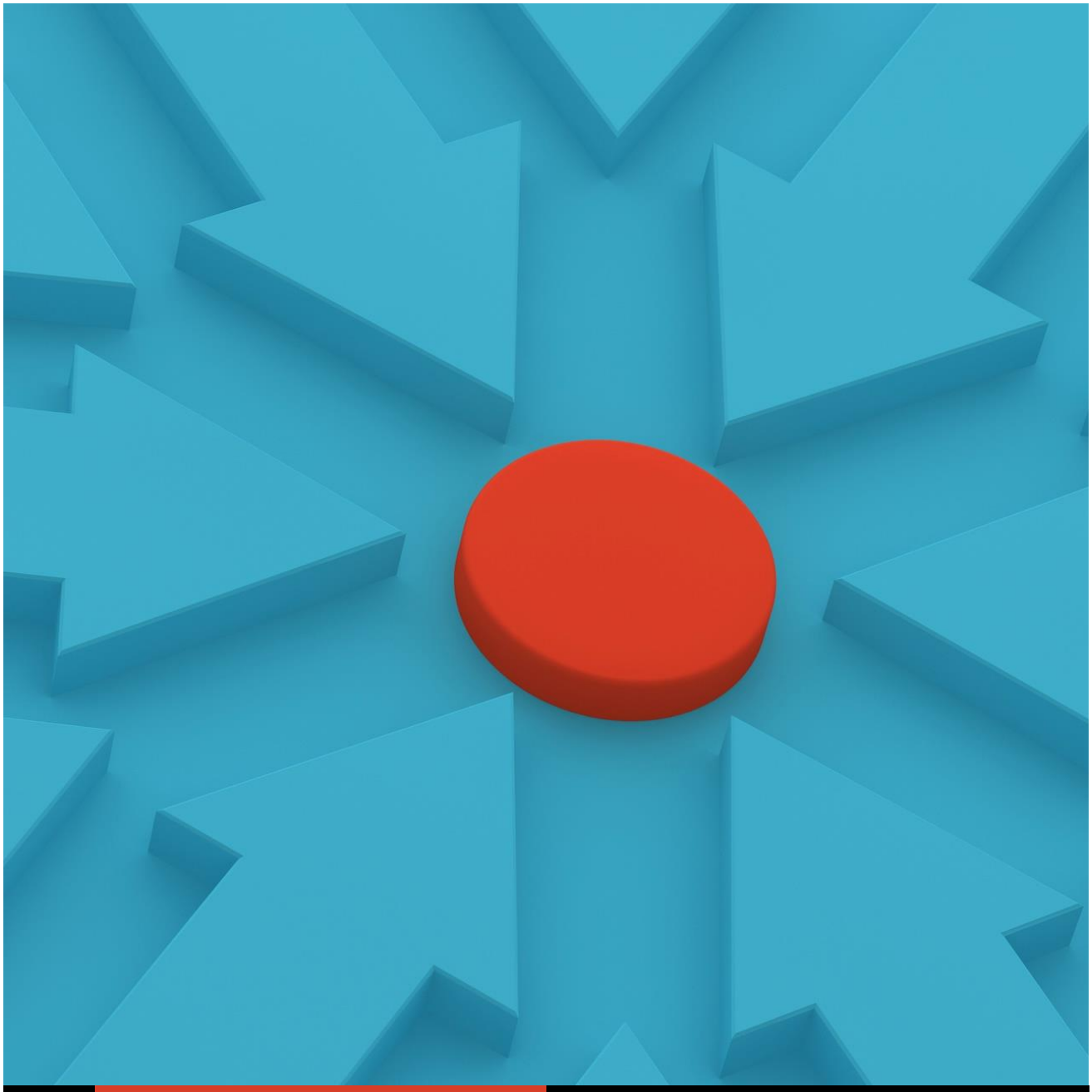
5.1 Effective Information Security and Information Governance assists the Council in protecting itself from cyber-attacks and security breaches, which can both give rise to service delivery and financial pressures. Measures of success therefore flow from demonstrated and continued compliance with all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

---

6. Supporting documents

6.1 Appendix 1 – SIRO Information governance – assurance & performance – 2019-20 and 2020-21 Report.

Katrina Hassell
Head of Business Solutions



SENIOR INFORMATION RISK OWNER (SIRO)

INFORMATION GOVERNANCE – ASSURANCE & PERFORMANCE: 2019-20 AND 2020-21 REPORT

NORTH LANARKSHIRE COUNCIL November 2021

Table of Contents

EXECUTIVE SUMMARY

This report provides an update relating to the responsibilities of North Lanarkshire Council's Senior Information Risk Owner (SIRO) and outlines activity and performance related to information governance. It provides assurances that information risks are being effectively managed; what is going well, and where improvements can be made. This report covers financial years 2019-20 and 2020-21, with details in respect of the 2019-20 year delayed to enable the SIRO to assess any additional requirements arising from deploying the new technologies envisaged within the Council's DigitalNL transformation programme.

INTRODUCTION

1. The Senior Information Risk Owner (SIRO) Annual 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 financial years 2019/20 and 2020/21.

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 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
      - Freedom of Information (Scotland) Act 2002,
      - Environmental Information (Scotland) Regulations 2004,
      - Public Records (Scotland) Act 2011, and
      - Information Security Standard ISO/IEC 27001:2013

   b. Outlines the 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

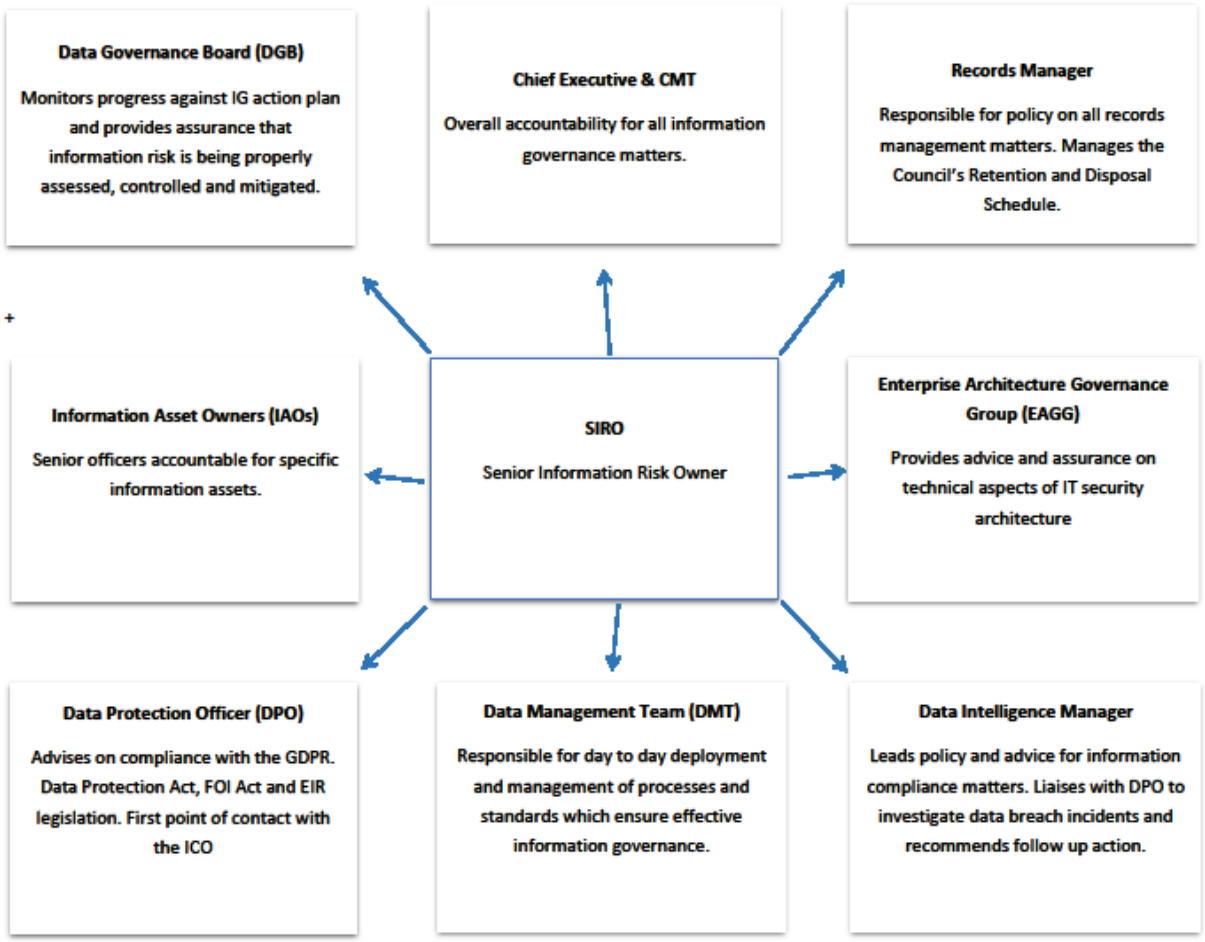
5. The Head of Business Solutions within the Chief Executive Office is the Council's Senior Information Risk Officer. Key responsibilities include:

   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. This report complements two annual reports prepared by the Head of Legal and Democratic Solutions. The first of these reports, presented to reflect the Corporate Data Protection Officer (DPO) responsibilities regarding data sharing, data breaches, Information Commissioner Office (ICO) Complaints and training in respect of financial years 2019-20 and 2020-21, were considered by the Finance & Resources Committee in May 2020 and November 2021 respectively. The second report, detailing Freedom of Information (FOI) and Environmental Information Requests (EIR) for financial years 2019-20 and 2020-21, were considered by the Finance & Resources Committee in November 2020 and 2021 respectively. To assist the Corporate Management Team and Audit and Scrutiny Panel in obtaining assurances in respect of 2020-21 information governance compliance, extracts of the DPO's reports are included where appropriate.

7. 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, processed appropriately and safely destroyed when not required.

8. 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, Records Manager, as well as the oversight responsibilities of the strategic Data Governance Board (DGB) and operational Data Management Team (DMT).



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 within the Data and Information Management Strategic Roadmap, and for ensuring measures are in place, through the Data Management Team, to monitor compliance with approved policies and standards.

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

11. The key Terms of Reference of the DGB include:

    a. To ensure the Council's information governance policies and management arrangements reflect current legislation, guidance/policies, and relevant professional codes of practice.
    b. To ensure that the Council undertakes or commissions annual assessments and/or audits of its information governance policies, procedures, and arrangements, with all findings included within improvement plans as appropriate.
    c. To receive the Annual Data Protection Officer report and scheduled internal audit reports, reviewing progress against required and identified actions as appropriate.
    d. To receive and consider reports into breaches of confidentiality and security and where appropriate undertake or recommend remedial action.
    e. To establish an information governance improvement plan, secure the relevant resources and monitor implementation of the plan.
    f. To 'sign off' the information governance assurance annual return and corporate information governance risk reviews prior to submission in line with the timetable issued each year.
    g. To promote a Council wide culture that information governance is the responsibility of all elected members and staff and to promote learning that arises out of investigations into breaches in information governance.
    h. To ensure that staff are trained in information governance, comply with, and understand the consequences of not adhering to relevant policies and procedures, monitoring the provision and uptake of such training in accordance with identified targets.
    i. To assist the Senior Information Risk Owner (SIRO) in producing information appropriate for inclusion within an annual Information Governance Report. Through this report, the Data Governance Board provides assurance to the Corporate Management Team and Audit and Scrutiny Panel.
    j. To ensure the Council develops and maintains an appropriate framework for the management and protection of information which is appropriately supported by information asset owners and administrators.
    k. To ensure the Council achieves positive movement on the data maturity curve, directing activities towards achievement of the 'advancing' stage of the maturity curve.

12. These Terms of Reference are reviewed annually to ensure the Group continues to meet the Council's business needs. The Terms were reviewed during 2020/21, with the focus of the DGB changed from service-based to functional to better reflect The Plan for North Lanarkshire, Council's transformation programme and the Data & Information Management Strategic Roadmap. Further details are outlined in paragraphs 66 to 72 below.

RISK MANAGEMENT AND ASSURANCE

13. 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 is ineffective. This includes implementation of enhanced and appropriate controls to address the additional information security and information governance risks arising from the significant shift to home working triggered by the Covid-19 pandemic*".

14. 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.

15. 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 Head of Business Solutions identified as the Corporate Risk Lead.

16. Throughout 2019-20 and 2020-21, this risk carried a residual risk assessment of 20, "*almost certain*" likelihood (5) and "*major*" impact (4) and was therefore monitored quarterly. The May 2020 review specifically examined whether existing risk controls and mitigations were sufficient to manage additional risks likely to arise because of the pandemic.

17. Reflecting the significant and fundamental changes deployed to the management and delivery of council services during the pandemic, the May 2020 review confirmed the likelihood of a breach was high, with additional controls and actions required to manage the additional risks arising from significantly increased numbers of staff working remotely. Such were identified and deployed, with the following highlighted to provide the Corporate Management Team and Panel illustrative examples of the additional measures put in place, and being managed and monitored, to avoid a breach and ensure information remains accurate and appropriately used.

Control (C) / Action (A)	***Description***
➢ CON0001054	Corporate and Service Business Continuity Plans in place and stress tested to inform priorities and decision making
➢ CON0001055	Increased suite of remote access concentrators to cope with and support increased numbers of remote users
➢ CON0001056	Guidance issued to managers and staff on home working which includes reference to data security
➢ CON0001058	Technical controls in place such as device authentication check, network-level user multi-factor authentication etc
➢ CON0001064	Secured Premises with secure storage and monitoring of security arrangements
➢ ACT0000610	Review current training content to ensure home working risks are identified in relation to information governance and expectations of staff are fully reflected

Control (C) / Action (A)	*Description*
➢ ACT0000603	Ongoing review and implementation of relevant new online collaboration and communication tools to maintain information security
➢ ACT0000604	Accelerate deployment of new digital packages including Microsoft Teams

18. The formal annual review of the Corporate Risk Register 2020-21 (December 2020) included a timetable for reporting corporate risks to the Corporate Management Team and Audit & Scrutiny Panel. Whilst accepting this is largely an improvement beyond the scope of this SIRO report, compliance with this recommendation saw this corporate risk subject to detailed scrutiny and oversight as follows:

	DGB	**CMT**	**A&S Panel**
Review Date	31/3/21	27/4/21	30/6/21

19. The DGB will continue to review controls and actions in accordance with the risk's residual risk rating, which is presently quarterly. Reporting to CMT and the Audit & Scrutiny Panel will be scheduled in accordance with the timelines recommended by the Audit & Risk Manager.

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 summarises the Council's data protection compliance for financial years 2019-20 and 2020-21.

Data Breaches

22. The Head of Legal and Democratic Solutions advised of the Council's data protection compliance and activity in his Annual Data Protection report to the Finance & Resources Committee in May 2020 (2019-20) and November 2021 (2020-21).

23. Paragraph 11(d) above illustrates numbers of breaches and near misses are reported to the Data Governance Board (DGB), with remedial and learning actions arising from investigations discussed to ensure clarity of change and/or requirement, with such subsequently cascaded council wide through the Data Management Team (DMT).

24. In financial year 2019-20, the Council recorded and investigated 67 potential data breaches, an increase of 8% on the previous year (62). This increase in recorded incidents was reflective of the picture nationally with all public bodies having taken action to ensure employees understood the data protection implications arising from the introduction of GDPR.

25. In financial year 2020-21, the Council recorded and investigated 49 potential data breaches. Whilst the DPO advises it is difficult to draw meaningful conclusion or trends, this 27% reduction on the previous year's figure of 67 could illustrate that the information governance arrangements outlined earlier (Diagram 1) are effectively cascading learning actions and a steady awareness of both data protection and information security requirements.

26. Chart 1 below compares recorded breaches from 2018-19 to 2021-22 YTD. The high volume recorded in November 2018 follows promotion of mandatory training on GDPR, so does indeed demonstrate that increasing – and then maintaining - awareness of personal responsibility on the use and protection of information better enables the Council to identify and address data breaches, near misses or information security incidents.

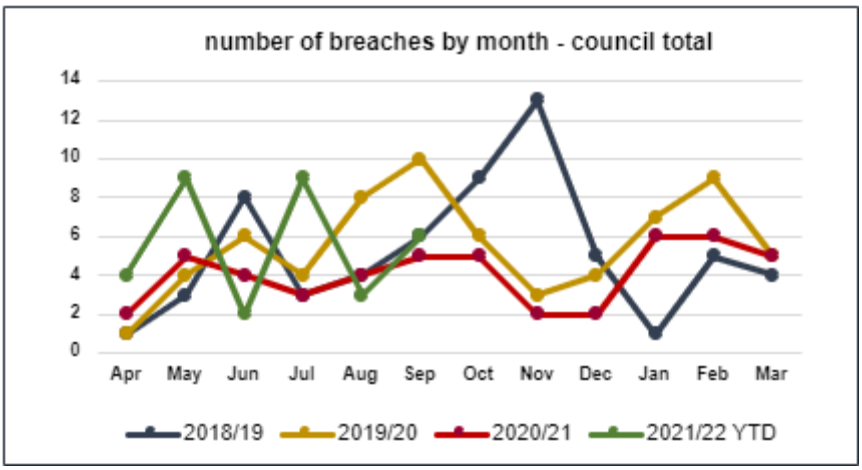


Chart 1

27. In investigating recorded incidents, consideration is given to whether such should be referred to the Information Commissioner's Office (ICO). Reportable incidents are considered to present a risk to the rights and freedoms of individuals, and for financial years 2019-20 and 2020-21, 12 and 4 incidents satisfied this threshold, and were reported accordingly.

28. Table 1 below analyses the 2019-20 and 2020-21 breach management and reporting position per council function, with Chart 2 comparing recorded breaches, per service, from 2018-19 to 2021-22 YTD.

Function	2019-20		2020-21	
	Recorded Incidents	Reported to ICO	Recorded Incidents	Reported to ICO
Chief Executive	20	3	13	0
Education & Families	24	3	16	0
Enterprise & Communities	14	3	10	1
Adult Health & Social Care	9	3	10	3
Totals	**67**	**12**	**49**	**4**

***Table 1**: Data breaches: 2019-20 and 2020-21*

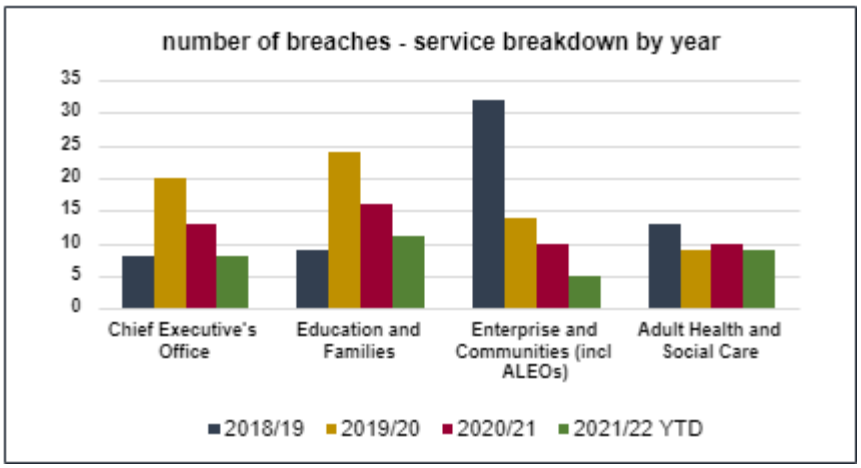


Chart 2

29. Categories of breaches include device/documents left in insecure locations, unauthorised system/app use, failure to redact data, wrongful disclosure of data and a break-in at the Civic Centre. 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 include reviewing existing policies, working towards a high completion rate for information governance training, and reviewing the security and procedures surrounding service use of mobile phones. All recommendations are included within the existing action plans of the DGB and DMT.

Subject Access Requests

30. Under the Data Protection Act and General Data Protection Regulations (GDPR) 2018, persons of all ages can request information about themselves – known as a Subject Access Request (SARs) - held by the Council. Lack of formal corporate procedures for handling SARs was identified as a key issue within the Internal Audit report of June 2019. Management acknowledged the need for more formalised and consistent reporting and tasked the former Information Management Working Group (now DMT) with implementing revised arrangements and tools. Effective December 2019, our corporate SharePoint platform now contains real time details of the numbers of SARs and compliance rates.

31. Acknowledging robust data is only available from December 2019, the Council received 23 SARs for financial year 2019-20, with 100% responded to within one month of receipt.

32. In respect of financial year 2020-21, 98 SARs were received. Of these, 61 (62%) were responded to within statutory timescales, with the pandemic contributing to this lower compliance rate due to frontline services having difficulty accessing manual documents during lockdown periods.

33. There is concern however regarding inconsistency of recording completion dates on the SARs SharePoint system, and of poor record-keeping regarding completed SARs within services. To minimize the risk of potential non-compliance within this area, the DPO plans to fully review existing support arrangements. This is therefore considered an area for improvement for 2021-22, with such reflected within the live action plan detailed within section 74 of this report.

Data Protection Impact Assessments (DPIAs)

34. DPIAs are used to identify the data protection risks of a project. They provide assurance that the Council is considering the data protection principles when designing processes which involve the use of personal data.

35. To satisfy the requirement to complete DPIAs, project Senior Responsible Officers (SROs) in consultation with Legal Service and Business Solutions, are required to complete a standard template.

36. In a report to the Corporate Management Team in April 2021, the DPO advised the volume of DPIAs has increased exponentially. This therefore increases the likelihood of ICO enforcement action being invoked should the Council fail to effectively complete DPIAs when required.

37. The DPO has further advised that the quality of DPIAs prepared to date varies, with many not being completed in accordance with the statutory requirement of Data Protection by design. A lack of training in this area to date combined with lack of clarity regarding responsibilities are acknowledged as the major contributory factors.

38. The Audit and Risk Manager confirmed through a 'reasonable assurance' rating in March 2021 that the Council has an effective approach to information governance. Recommendations were made however regarding low levels of mandatory training. Recognising DPIA training has also been identified as an immediate requirement by the DPO to ensure GDPR compliance, significant activity must be undertaken during financial year 2021-22. Paragraph 74 below provides some commentary in this regard.

COMPLIANCE WITH FREEDOM OF INFORMATION (FOI) AND ENVIRONMENTAL INFORMATION REGULATIONS (EIR)

39. During 2019-20, the Council received 1,536 requests for information under the Freedom of Information Act and the Environmental Information Regulations. This consisted of 1,261 FOI requests and 274 EIR requests and represents a decrease of 7% compared with 2018-19 figure of 1,652.

40. Nineteen requests were either withdrawn by the requester or closed during the process following clarification. Of the remaining 1,517 requests progressed, the Council responded to 97.8% (1,483) within the statutory deadline. Though marginally lower than previous years (98.2% in 2018/19, 98.5% in 2017/18), a response rate of 96% and above is considered excellent within the Scottish Information Commissioner's Self-Assessment Toolkit for Public Authorities.

41. Lower performance in 2019-20, and particularly quarter 4 (94.7%), is largely reflective of the March 2020 lockdown, with staff initially having delayed access to information as they transitioned to remote working.

42. Customers who submit a FOI or EIR can request an internal review if they are not satisfied with the response provided. Full details of all requests received, the category of applicant,

and cases submitted for internal review are outlined within the Head of Legal and Democratic Solutions annual reports to committee (para. 6 above.)

43. By way of summary however, 36 requests (2.3%) for internal review of the original decision were received in 2019-20. Of this 36, the original decision was upheld wholly or partially in 24 cases, 9 were overturned and received a new decision at review, with 3 reviews undertaken due to there being no response sent to the original request.

44. If an applicant is not satisfied with the outcome of an internal review, they can refer their case to the Scottish Information Commissioner (SIC), who will assess the case and make an independent decision on how the Council has handled the request. In 2019-20, following internal review, 4 cases were appealed to the Scottish Information Commissioner. Three of these appeals were withdrawn during the appeal process, with the final appeal finding in favour of the requestor.

45. In financial year 2020/21 North Lanarkshire Council received 1,245 requests for information. This consisted of 987 FOI requests and 258 EIR requests and represents a 19% decrease on the 2019/20 total of 1,536 requests. In his paper to Finance & Resources Committee (November 2021), the DPO states this is the lowest total number of requests received since 2012/13.

46. Of the 1,245 requests received during 2020/21, 23 requests were not fully progressed. Of the remaining 1,222 requests that were fully progressed 1,164 (95.3%) were responded to within the statutory 20-day deadline. This is lower than the compliance rate (97.8%) achieved in 2019-20 and is largely because of the pandemic, particularly in the first quarter of the year when the Council was adjusting to staff working from home and prioritising core service delivery over FOI.

47. For 2020-21, 22 (1.77%) requests for internal review of the original decision were received. Of this 22, the original decision was upheld wholly or partially in 17 cases with 3 decisions either overturned or considered non-compliant. One internal review was withdrawn by the requester and one review was undertaken because there was no response to the original request.

ICT SECURITY AND CYBER RISKS

48. 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.

49. The Council complies with the requirements of the Scottish Government Cyber Resilience Framework by having the Head of Business Solutions, 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. To mitigate against cyber risks, the Council follows published NCSC guidance and adopts the following approaches:

a. Full compliance with the externally inspected Public Sector Network (PSN) accreditation via submission of the required IT health check applications, and implementation of all recommendations subsequently identified as potentially high risk. Our next accreditation submission date falls due in January 2022;
b. Planned compliance with the Payment Card Industry Data Security Standard (PCI DSS) accreditation, with a detailed project underway to fully achieve by March 2022;
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;
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 and compliance monitored by the Council's service delivery partner, Wipro;
f. Robust authentication and access control procedures e.g.: multi-factor authentication, in place to protect Council systems from unauthorised access, with such now of significance given the increase in home and mobile working by individuals in response to the Covid-19 pandemic;
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.

50. The Council also held a Cyber Essentials accreditation between 2018 and 2020. Cyber Essentials is a Government-backed industry-support scheme designed to help organisations to protect themselves against common cyber-attacks. The Audit and Risk Manager advised the Panel in March 2021 that the Cyber Essentials certification had lapsed and should be re-instated as soon as possible. Business Solutions submitted the application to an appropriate external specialist towards the end of 2020-21, but the Council failed to meet the more onerous compliance requirements of this external accreditation.

51. With compliance standards now including requirements to for example, fully transition to supported tools and deploy all updates/patches within 14 days of release, achieving compliance is now cost prohibitive for the Council. To provide some context, the council's technology network presently includes 530 servers, circa. 200 server software/applications and approx. 1,500 different desktop/device types of software. Whilst the Council's DigitalNL transformation programme will see us fully transition all products to more modern cloud hosted solutions, such cannot be achieved overnight. Given business critical systems such as MySwis and eFinancials rely on older – and often unsupported – software and applications, there is no scope for the Council to now satisfy all Cyber Essentials standards. Like many other public sector organisations, Business Solutions has determined Cyber Essentials cannot meet our needs and will therefore largely seek to protect itself from common cyber-attacks through our PSN accreditation and regular threat assessments.

52. Over the course of 2020-21, Business Solutions sought to further improve its information security arrangements, planning through a Security and Risk Management Workshop, to identify our existing Information Security Maturity Assessment (IT Score) and

consequential priority improvement actions. Competing priorities to support home working and the digital transformation programme impacted key attendee availability, with the initial workshop cancelled various times before eventually taking place virtually in January 2021.

53. Measured on a scale ranging from 1 (low or not important) to 5 (high or most important), this maturity score tool assesses how well the Council's activity compares with Gartner's best practice research. The tool examines 30 different activities over 7 categories to assist an organization to prioritise effort and improvement activity to reflect business need and objectives. Having completed the assessment, Business Solutions has included (a) develop a controls catalogue, (b) monitor, manage and remediate risk exposure, and (c) documenting and managing the implementation of the technical plan as the key activities for the Information Risk and Security and ICT Infrastructure teams within the live action plan detailed within section 74 of this report.

54. In 2020 the Council participated in the National Records of Scotland's voluntary Progress Update Review mechanism in relation to its records management arrangements as laid out in its Records Management Plan (RMP). The Public Records (Scotland) Act 2011 Assessment Team commended the Council for undertaking voluntary self-assessment and reporting on its RMP.

55. The Assessment Team's findings considered that the Council continues to take its statutory obligations seriously and is working hard to bring all elements of the Records Management Plan into compliance with the Act. These findings have been published on the National Records of Scotland website. *NRS - Progress Update Review (PUR) Final Report by the PRSA Assessment Team for North Lanarkshire Council and Licensing Board, February 2021 (nrscotland.gov.uk)*

56. The expectation is that the Council will be invited to develop and submit a new Records Management Plan in 2022 however this may be pushed back as determined by the Assessment Teams own schedule.

CORPORATE GOVERNANCE ACTIVITY

57. The Council is committed to a clear strategy and sustainable framework for information governance and security, so refreshed its corporate working arrangements in December 2019. The Data Governance Board (DGB) replaced the Information Governance Working Group (IGWG) with the Data Management Team (DMT) also replacing the Information Management Working Group (IMWG).

58. With both groups established to develop, implement, and ensure compliance with data governance and management strategies, policies, and standards, the DGB and DMT have responsibility for continuously monitoring the actions required to manage information issues, risks, and cultural behavior to improve existing data governance and management. This section of the report details activities undertaken during 2019-20 and 2020-2021 to strengthen the Council's management of information risks.

59. Paragraph 11(h) above specifically references the importance of information governance training, with such identified as an area for improvement within the June 2019 Internal Audit report. Whilst various steps were taken throughout 2019-20 and 2020-21 to refresh, promote and monitor completion of mandatory Data Protection Essentials, Records and Information Management and Information Security training modules, the low uptake of

these mandatory modules remained as an identified improvement area within the Information Governance Internal Audit report presented to the Audit and Scrutiny Panel in March 2021.

60. This recommendation is expected given COVID-19 priorities resulted in work to identify posts which must complete the mandatory training modules – planned for 2020-21 following the launch of the new LearnNL system – being postponed. Such is vital however for the DGB to certify, through the Data Management Team, that all required staff remain compliant with their mandatory training requirements. This therefore features in the live action plan detailed in section 74 of this report.

61. Though acknowledging further work is underway to improve performance monitoring, three performance indicators were developed during 2020-21 for monitoring completion of the mandatory information governance training courses in LearnNL. Chart 3 below details the level of completions, per service, for each of the mandatory modules following their relaunch, as well as the discretionary Data Protection Advanced training module.

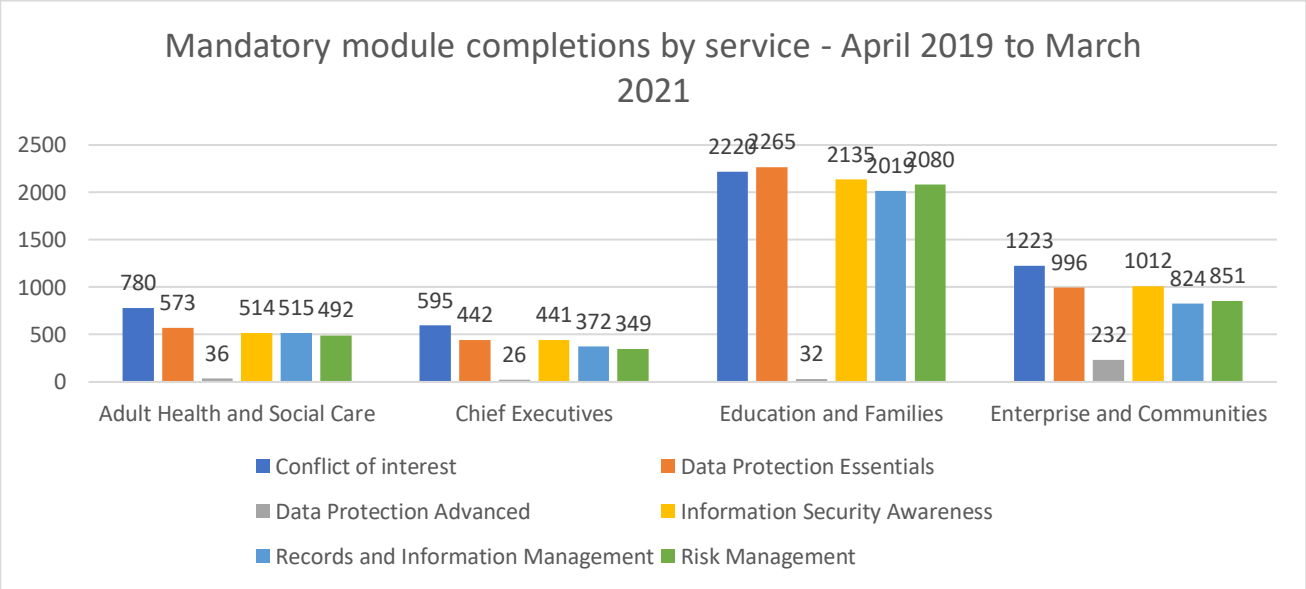


Chart 3

62. Chart 3 illustrates that for the 2-year period to 31st March 2021, over 5,000 employees completed the mandatory courses, with "attendance" at each of the courses largely consistent per service. Given mandatory modules need to be completed biennially, this information forms the starting point firstly for the DGB to gain assurances that staff are being trained in information governance, and secondly, to assess the impact which planned improvements regarding performance monitoring have had.

63. Chart 4 below presents a further analysis of training undertaken during financial year 2020-21, with very low levels council-wide evident during those early months of the pandemic. Promotion of modules by DGB and DMT members, regular NLC email announcements and events such as the annual Information Management Week do appear to be successful, with numbers substantially increasing from September 2020 onwards. Section 74 below illustrates that awareness raising and GDPR promotional compliance remains as a key activity on the information governance improvement action plan for 2021-22.

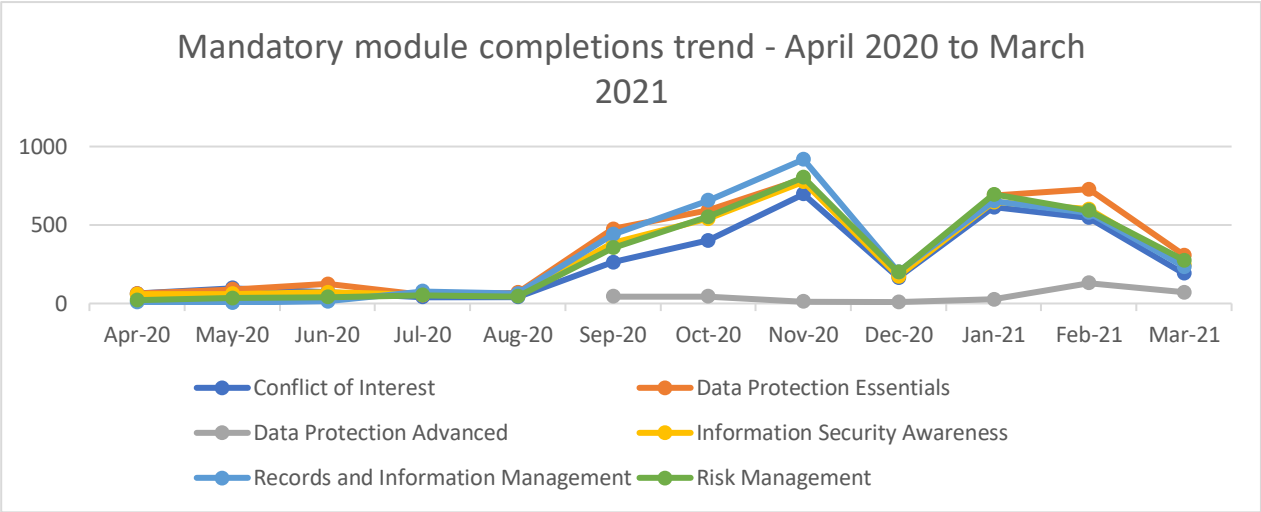


Chart 4

64. Paragraph 30 above illustrates significant improvements have been made regarding the handling and reporting of Subject Access Requests (SARs), with the Council's SharePoint platform now containing real time details of SARs and compliance rates. Such appears insufficient however to ensure the council is complying with its legal obligations, and to that end, several actions are required, with such included in section 74 of this report.

65. As outlined in paragraph 57 above, the Council refreshed its corporate information governance arrangements following Policy & Strategy Committee approval of the Digital & IT Strategy 2019-2023. The refreshed arrangements commenced in January 2020, with members of both groups given opportunity to raise their awareness of the Digital & IT Strategy, existing information governance policies, and the DigitalNL transformation programme. Reflecting a recommendation within the June 2019 Internal Audit report, the governance groups were thereafter tasked with completing an interim review of the Information Governance Policy Framework and associated suite of information governance policies. A full biennial review of the Information Governance Policy Framework followed during 2020-21, with details presented to the Policy and Strategy Committee on 3rd June 2021.

66. During 2019, the Council commissioned its Digital Business Partner (DBP) to assess the capacity of its existing information management (IM) and data governance processes to deliver against the data-driven decision-making model envisaged by The Plan for North Lanarkshire ("The Plan"). The key deliverable from this engagement was a Data and IM Strategic Roadmap (the Roadmap), approved initially at Corporate Management Team (CMT) in September 2020, and subsequently endorsed by the Transformation and Digitisation Committee on 24th February 2021.

67. In finalising the Roadmap for CMT and Committee consideration, feedback was sought in the first instance from the Organisational Design Authority (ODA) sub-group of the DigitalNL Delivery Board. With comments suitably included, the Roadmap was thereafter issued to the Data Governance Board (DGB) in March, June, and August 2020 respectively to facilitate an opportunity for this strategic governance group to shape the Roadmap for CMT deliberations.

68. In approving the Roadmap, CMT also approved a strategic vision for data and a revised Data Governance and Management Framework. The strategic vision for data, illustrated graphically in chart 4 below, envisages a core Business Intelligence Hub being developed to transition the Council from its existing 'basic' data maturity score to an 'advancing' score, and all data being virtualised and available as 'a single view'; firstly to assist services in monitoring performance against The Plan for NL outcomes, and secondly, to support strategic decision making, service delivery, cost reduction and risk management arrangements.

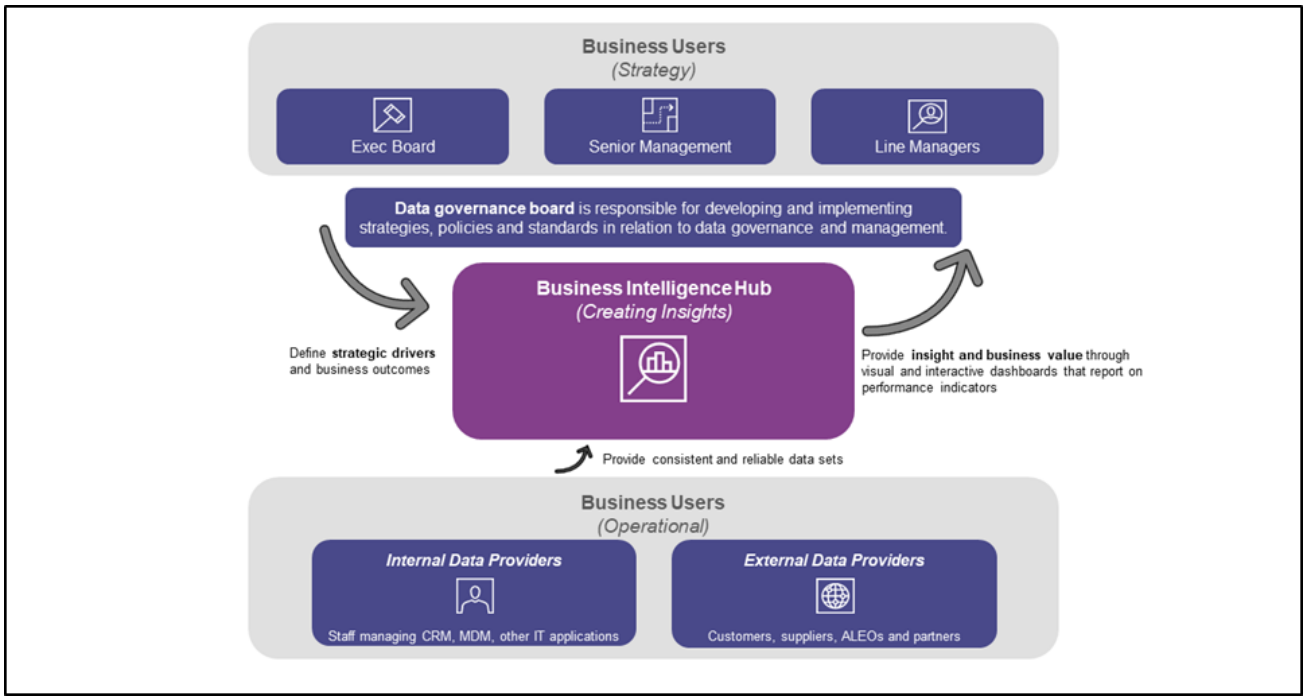


Chart 4: Strategic Vision for Data

69. The Roadmap, presented as a series of work packages, provides opportunity to facilitate an incremental improvement in the Council's data maturity score. To enable the Council to establish clear timelines for the transition, the Corporate Management Team:

    a. Confirmed DGB membership would change from service specific representation to functional master data representation. This change became effective at the DGB meeting of 9th December 2020, with Business Data Owners identified for the key master data entities of customers, cases, people, and organisation.

    b. Endorsed development and progression of a Data Custodian Model. Consultation on this has commenced through various corporate working groups, but most of the activity is expected to be managed and governed through the DGB and ODA sub-group of the DigitalNL Delivery Board.

70. The Transformation and Digitisation Committee reviewed the roadmap progress in February 2021, noting such would be driven forward through the DGB over an envisaged 3-year timeframe. Regular reporting of progress against the strategic data roadmap to Committee is included within Business Solutions' Programme of Work for 2021-22.

71. A move to a Data Custodian model necessitates a further review of the Terms of Reference of the DGB and DMT to ensure such is effectively aligned with, and capable of delivering against, the approved Data Governance and Management Framework. The

DGB review commenced at the meeting held on 31st March 2021, with sign-off of revised terms achieved at the next group meeting in May 2021.

72. Whilst further detail regarding deployment of the Data Custodian model is largely beyond the scope of this report, it is worth highlighting that the roles of Business Data Owner and Data Steward are defined and available to services to enable them to consider how such should be reflected within their ‘Delivering for Communities’ structures from April 2022.

LIVE IMPROVEMENT PLAN

73. Paragraph 11(e) above highlights the DGB Terms of Reference require the group to establish, resource and monitor an information governance improvement plan. Such an action plan is maintained, and outlines key tasks required, together with details of the responsible officers, completion timescales, current status and percentage complete. The plan is monitored by the DMT and is a standing agenda item at meetings of the DGB, enabling progress updates and escalation of specific tasks as required.

74. By its nature, the plan must be flexible and dynamic, with any new improvement areas identified by for example services, Business Data Owners, management, and Internal Audit appropriately incorporated. The following represents a summary of the key actions included within the improvement plan at March 2021. It is envisaged these will be progressed throughout 2021-2022 to further strengthen the Council's information governance and data accuracy arrangements:

a. Raise the profile and prioritisation of Information Governance and Data Protection responsibilities

- Through the corporate SharePoint platform, services now have access to real time details of SARs quantities and compliance rates. Many staff involved in the process are however not recording completion dates on SharePoint, which results in compliance presently being based on a manual interrogation of the system.

- Mandatory online training modules for information governance and security were refreshed and launched on the LearnNL online training platform during 2020. Completion rates for the last 2 years detailed in sections 61 and 62 above remain lower than desired however, and therefore require awareness raising to remain as a key priority on the information governance improvement plan. Such activity will also consider appropriate training in respect of DPIA and privacy notices.

- Reflecting the Target Operating Model (TOM) approved by the ODA and Digital NL Delivery Board during 2019-20, the DPO will develop and present to the DGB potential options for improving the awareness and compliance of SAR and DPIA responsibilities.

b. Refresh approach to mitigating Cyber Security risks

- The Cyber Essential external accreditation, which aims to support organisations to protect themselves against common cyber-attacks, is now considered cost prohibitive for public sector organisations. The Council must demonstrate it has appropriate arrangements in place to manage cyber risks and will now do so as part of planned PSN accreditations and threat assessments.

- Based on the findings of the Information Security Maturity Assessment (IT Score), we will look to implement these improvement actions during financial year 2021-22: a) develop a controls catalogue, (b) monitor, manage and remediate risk exposure, and (c) documenting and managing the implementation of the technical plan.

c. Map Mandatory and Discretionary Training to Roles

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

- With LearnNL launched summer 2020 and a Data Custodian model approved by the CMT and DGB during 2020-21, it is essential all future information governance and security training – particularly for staff - be tailored to suit the needs of individual posts.

- Though the existing mandatory and discretionary modules are anticipated to remain, additional discretionary training, linked to the new requirements associated with Business Data Owners, Data Stewards and Data Architects, will be required.

- The Business Data Owner for the 'people' data entity (Employee Service Centre Manager) and Relationship Manager within Business Solutions will work with services as a priority to identify posts required to complete mandatory information governance training modules. Both will also work with the Talent and Organisation Development (TOD) team to identify training to appropriately increase the awareness of other roles and elected members regarding their responsibilities to ensure information and data is held securely, processed appropriately and safely destroyed when not required.

d. Incremental implementation of the Data and IM Strategic Roadmap (the Roadmap)

- Section 69 above illustrates the Roadmap will be implemented through a series of work packages. Given the inherent links to the DigitalNL Programme and developing Business Intelligence Hub, aspects of the Roadmap are already underway. Other aspects will be taken forward incrementally through the DGB and DMT, with detailed timescales for delivery established.

- The new Data Governance and Management Framework is essential for ensuring data is viewed and used as an asset council wide. This, and the associated Data Custodian, Data Steward and Data Architect roles, will be further defined, developed, and deployed within services through the refreshed DGB and DMT arrangements.

- DGB and DMT Terms of Reference to be further reviewed to ensure effective alignment with the approved Data Governance and Management Framework. DMT membership to vary to ensure Data Steward representation adequately reflects all key Line of Business (LOB) systems, with joint work between services and Business Solutions planned to identify all key LOB.

CONCLUSION

75. In summary, significant progress was made during 2019-2020 and 2020-2021 to strengthen the Council's approach to managing its information risks, with sections 48 to 72 above providing relevant context and detail.

76. 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 (March 2021), this subject matter remains a high priority improvement area for the Council.

77. A detailed improvement plan exists and is monitored by the DMT. A summary of the priority actions at March 2021, is detailed above. Progress against these will be managed by the DGB throughout 2021-22, 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.

Katrina Hassell
Head of Business Solutions