North Lanarkshire Council
Report

Audit and Scrutiny Panel

☒approval ☒noting **Ref** KH/RL/CM **Date** 30/06/21

Information Security and Information Governance Risk

From **Head of Business Solutions**

E-mail HassellK@northlan.gov.uk **Telephone** 07903 096121

Executive Summary

To support the Council in mitigating risks and uncertainty, all services operate risk management arrangements which identify, evaluate, manage, and control a range of key corporate risks.

This report focusses on the Information Security and Information Governance risk and provides the Audit and Scrutiny Panel with an update of measures to address this risk, which the Panel will remember carries a high residual score. The report provides an overview of existing controls and actions taken to date, and illustrates further actions planned to continue to manage this risk.

Recommendations

It is recommended that the Audit and Scrutiny Panel:

1. notes the actions taken to date to manage the Information Security and Information Governance Corporate Risk;
2. notes the on-going actions to manage this risk as detailed in paragraphs 2.5 to 2.9; and
3. approves the next actions proposed as detailed in paragraphs 2.10 to 2.16.

The Plan for North Lanarkshire

Priority All priorities

Ambition statement All ambition statements

1. Background

1.1 The council is entrusted to manage data, including sensitive or 'special category' data, for the benefit of service users. It must do so in accordance with statutory responsibilities which include but are not limited to the Data Protection Act 2018, Freedom of Information Act 2002, Public Records (Scotland) Act 2011 and General Data Protection Regulations (2016).

1.2 If information is not available, is corrupted, or is inappropriately released, the council may be unable to deliver critical services or comply with its legal obligations. To this end, various reports regarding the Council's information management arrangements and associated risk assessments have previously been considered by the Audit and Scrutiny Panel.

1.3 The Information Security and Information Governance risk covers the council's management of data in all formats e.g. paper records, official documents, electronic, multimedia, conversations etc. Notwithstanding this, although all data is covered by this risk the focus is on digital data as most business-critical data is now created, processed, and stored digitally.

1.4 Factors which impact on digital data risk include:

- The increasingly interconnected nature of digital networks and adoption of new technologies (such as the Internet of Things) mean new threats are omni-present and distance is no longer a barrier to threat actors.
- The rapid adoption of new ways of working, such as making use of home, remote and agile workplaces, as well as the use of third parties to process council information, has changed the threat landscape considerably in comparison to only a few years ago.
- It is recognised events of global magnitude and with enormous social, economic and health implications can occur. These events have both a direct impact on the council's ability to effectively govern and secure its information, as well as an indirect impact through driving change in how information is processed.
- New legislation and regulation with which the council is expected to comply is being continually created and revised e.g.: draft Adequacy Decision (February 2021). Adherence to these will consume resource, and non-adherence or breach may result in even more cost impact.

1.5 The Covid-19 pandemic has resulted in a rapid move to home working, bringing with it challenges to information security and information governance. These are exacerbated by hostile actors targeting home workers during the pandemic. The increased uptake in home working has also resulted in council premises having no or reduced staff presence which has implications for the security of data stored in such locations.

1.6 This risk remains as the joint top risk on the council's corporate risk register and, as such, has been subject to significant action in terms of reducing both the likelihood of the risk occurring and the impact should an event take place. This activity together with on-going and proposed future activity is detailed in this report.

2. Report

2.1 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. On applying mitigation measures the residual score reduces to 20 (likelihood of 5 with impact reducing to 4), resulting in this being one of four significantly high corporate risks.

2.2 The risk that information, in whatever format, is not managed securely or that information governance across the Council and its ALEOs is ineffective must be robustly addressed and effectively managed. This includes implementation of enhanced controls which address the additional information security and information governance risks arising from the significant shift to home working triggered by the Covid-19 pandemic.

2.3 The list of factors that contribute towards this risk can be long. The following is a high-level summary of the principal generic factors that influence this risk across all industries, and are reflected in the Information Security and Information Governance risk:

- Technical (preventive/detective/corrective) controls applied to ICT systems.
- Information governance arrangements.
- Policies, standards, procedures, and audit processes.
- Staff awareness of, and adherence to, good security practice.
- Physical security arrangements.
- Changes to ways of working:
    - Adoption of "the Cloud" to process information.
    - Increase in the number of empty offices which may contain information.
    - Management of confidential information by home workers.
    - Disposal of confidential waste (including homeworkers).
    - Remote access to ICT facilities (including home workers' laptops).
- Changing threat landscape:
    - Increasing capability of threat actors – many of which are state sponsored.
    - Prevalence of digital fraud.
- Resource challenges e.g. a lack of skills and knowledge across organisations with regards to managing information risk.
- Changes to legislative, regulatory and compliance portfolios and requirements.
- Recognition that external events which create sudden and significant shifts in the way technology is used do happen.

2.4 The impacts of a breach can be significant. Should an event occur these can include:

- Adverse media coverage and reputational damage.
- Breaches of information resulting in significant fines from regulatory bodies.
- Litigation.
- Considerable resources being required to remedy issues and areas of business negatively affected.
- Inability to comply with statutory requests within set timescales.
- Harm to individuals (especially where the council has a duty of care).
- Loss of vital or historical records, and
- System outages.

2.5 To address this risk the council has undertaken considerable activity to reduce, where possible, the likelihood of an event occurring and, if it does, the severity of the impact. Actions have been undertaken and controls put in place including:

- Governance Boards and Groups to manage information and the use/adoption of ICT:
    - Data Governance Board
    - Data Management Team
    - Enterprise Architecture Governance Group
    - Technical Design Authority
- Appointment of a Data Protection Officer and supporting team to ensure compliance with provisions of the Data Protection Act 2018 and UK GDPR.
- Implementation of a SARS recording and monitoring process.
- Creating and ensuring regular review of a council-wide Information Governance Policy Framework.
- Records Manager advises on compliance and supports creation of a records' management plan inc. information retention schedule.
- Corporate and Service business continuity planning.
- Appointment of an Information Risk Manager and supporting team.
- Implementation of an evolving suite of cyber-controls to prevent system outages whether accidental or malicious.
- Generic mandatory security awareness training delivered to all staff.
- Wider security awareness, including management of risks associated with new ways of working, being made available to staff through a variety of channels.
- Improved supply chain security assurance.

2.6 The council is no exception to the rule that organisations must continue to develop their security posture to address the changing threat environment. Activities are on-going to maintain and enhance the council's information security and information governance measures and these range from technical to process, procedural and staff awareness raising.

2.7 In terms of governance, the Data Governance Board (DGB) provides a cross service strategic platform to address information management issues and ensure that lessons are learnt from breaches and near misses. In addition to the DGB the Data Management Team (DMT) provides a cross service operational platform to:

- Raise compliance awareness.
- Address operational information management issues and focus on ICT Security related compliance.
- Establish short life sub-groups to progress specific tasks.

2.8 Supporting the work of the DGB and the DMT the council has implemented an Information Governance Policy Framework which brings together the council's information governance policies and ensures that they operate effectively. This framework undergoes regular review and includes guidance for staff on the implementation of relevant policies e.g. Information Security Policy and Acceptable Use of ICT Policies. The council has appointed an Information Risk Manager who leads a small, newly formed, Information Security Team.

2.9 Technical activity that is on-going includes laptop and mobile storage device encryption, secure file transfer via Hyve, e-mail encryption, enhanced anti-virus software adoption, network segmentation, penetration testing, and multi factor authentication roll out. In addition, over 1,600 headsets have been distributed to staff to help maintain a degree of call privacy when working from home.

2.10 As stated earlier, the threat environment that the council must address rapidly evolves. This, combined with the large number of staff working at home, will require further technical, procedural, and staffing awareness initiatives to help the council manage the risks associated with information security and information governance. A full review of the training framework is planned following full roll out of M365.

2.11 Future technical and administrative/procedural initiatives and solutions will always be required to be built on what has already been established. A pipeline of activities is planned that includes making improvements to disaster recovery planning and testing arrangements, managing supply chain security, ensuring robustness of authentication processes for users, creating a secure development operations framework, and enhancing joiners/movers/leavers processes. An effective means of performing technical vulnerability management is also on the security roadmap.

2.12 Security needs to work for people. The council must continue to develop security measures that support and assist staff to undertake their job and ensure that it does not hinder them as they undertake daily tasks. Staff will also need to have high levels of cyber and information security awareness and this knowledge will need to be regularly updated. Staff awareness levels cannot be assumed – they will need to be assessed. To support staff in raising their awareness the Information Security Team will build on its recent staff awareness raising e-mails sent out during Cyber Security Week in February 2021. A basic yet significant improvement is raising and reinforcing awareness of how not to be a victim of cyber fraud, which is probably the single most common root cause of ransomware attacks.

2.13 In addition to, and supporting, the staff awareness campaign the Information Security Team will assist in the review of existing mandatory data protection courses with a view to updating these and enhancing aspects relating to information security and cyber security. Uptake is monitored quarterly by the DGB.

2.14 To further support the on-going response to information risk and need for appropriate information governance controls to be in place internal standards will be developed and adopted. These will form the bedrock of good practice to be followed by internal ICT teams as well as, where applicable, users more widely. Topics will include user endpoint and server security, application of cryptography, user and device authentication, equipment disposal, and privileged access management. The Information Security Team will provide a lead in developing these standards and support the council in their adoption as appropriate.

2.15 A suite of compliance activities is currently under way, including against the Public Sector Network Code of Connection, Cyber Essentials, and Payment Card Industry Data Security Standards. Local authorities are by their nature complex, and many authorities in Scotland have determined that meeting the requirements of all these frameworks is not pragmatic or cost effective.

2.16 Measures to support home working in the pandemic have already been undertaken as have measures to secure buildings and the information that is stored in them while they remain under or unoccupied. As the council transitions out of the pandemic it is likely that many former office-based staff will become workers that are predominantly home-based. Longer term, sustainable approaches to supporting information security and information governance will need to be developed including addressing issues such as printing, disposal of confidential waste, etc. The Information Security Team

will work with IT staff to ensure that the right technical approach can also be the right security approach.

3. Public Sector Equality Duty and Fairer Scotland Duty

3.1 Fairer Scotland Duty

The requirement to comply with The Fairer Scotland Duty does not apply in this case.

3.2 Equality Impact Assessment

The details of current and proposed future activity with regards information security and information governance should have no impact on the council's duties under the Equality Act 2010 Public Sector Equality Duty Regulations.

4. Impact

4.1 **Financial impact**

Effective information security and information governance can assist in ensuring the council does not incur fines (up to 4% of turnover per event) for breaching UK GDPR requirements and can also minimise costs associated with service interruptions and restoration of lost data. To this end, sufficient resources must be made available to satisfactorily maintain the activities detailed in this report. Procurement of appropriate technologies is provided for within the approved Strategic Capital Investment Programme 2021/22 to 2025/26, with the staffing costs of the Information Risk Management team funded through Business Solutions revenue budget.

4.2 **HR policy / Legislative impact**

Delivery of effective information security and information governance is essential in fulfilling the Council's statutory obligations.

4.3 **Technology / Digital impact**

Technology / digital impacts will be significant as security aspects will be required for all technology procured and digital solutions used. These costs should be identified at the commencement of any project and included in the procurement exercise (and budgeted for accordingly).

4.4 **Environmental impact**

There are no negative environmental impacts to the report however it should be noted that enhancing technology including the ability to work from home should lower the council's overall carbon footprint.

4.5 **Communications impact**

There will be an on-going need for communication and consultation with key stakeholders and staff to ensure that this risk continues to be effectively managed over time.

4.6 **Risk impact**

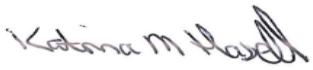
If the council does not effectively address this risk then there are considerable risks to the council in terms of reputational damage, loss of service (and significant costs to restore service), loss of confidence amongst staff and stakeholders and the possibility of very significant fines should we fail to deliver any of our legislative and statutory responsibilities.

5. Measures of success

5.1 The continued effective management of this risk with security breaches being minimised in terms of number and severity, service disruption being minimised, and, in addition, higher sustained levels of staff awareness will be key measures of success.

6. Supporting documents

6.1 Appendix One – Information Security and Information Governance Deep Dive.



Katrina Hassell
Head of Business Solutions

Appendix 1

Deep Dive Report RIS0000019	**Risk Title** Information security and information governance	**Owner** Katrina Hassell

Risk Context

NLC is entrusted to manage data, including sensitive or 'special category' data, for the benefit of service users. If this information is not available, is corrupted, or is inappropriately released, the Council may be unable to deliver critical services or comply with our legal obligations. This risk covers the Council's management of data in all data formats e.g. paper records, official documents, electronic, multimedia, conversations etc. That said, the focus of this risk is digital: our vital records are now nearly all created and processed in that format and although we won't ignore face-to-face spoken and paper information, the potential for and impact of loss of digital information, as well as of our electronic and digital processing systems, mean they have to be our primary concern. Factors which contribute to this risk include:

i)The increasingly interconnected nature of digital networks and adoption of new technologies (such as the Internet of Things) mean new threats are omni-present and distance is no longer a barrier to threat factors;

ii)The rapid adoption of new ways of working such as rapid adoption of home, remote and agile working as well as the use of 3rd parties to process council information has changed the threat landscape considerably in comparison to only five years ago;

iii)It is now recognised events of global magnitude and with enormous social, economic and health implications can occur. These both have a direct impact on our ability to effectively govern and secure our information, as well as an indirect one through driving change in how information is processed.

iv) New legislation and regulation with which the council is expected to comply are continually being created and revised. Adherence to these will consume resource, and non-adherence or breach may result in even more cost impact. For example, The General Data Protection Regulation (GDPR) implemented on 25th May 2018, raised potential for fines up to 4% of turnover or 20,000,000 euros whichever is greater.

The UK left the European Union on 1 January 2021 and from that date is no longer a member of the European Economic area, which is the collection of states covered by the terms of the GDPR. The Data Protection Act 2018 has been amended and has effectively become the UK GDPR. It was agreed that, as part of the Withdrawal Agreement, the European GDPR will remain in force for a period of four months with a possible further two-month extension. This is primarily to allow for an adequacy decision to be made by the European Commission in relation to the UK, i.e. whether the UK will be deemed to have adequate safeguards in place to adequately provide standards similar to those imposed by European GDPR. This will have a significant outcome as to whether data processors based in Europe would have confidence in exporting (or returning) personal data which they hold to organisations within the UK. On 19 February 2021, the European Commission published a draft adequacy decision in favour of the UK. This is effectively a finding that the UK is deemed to have equivalent data protection safeguards in place as those imposed by European GDPR. Final confirmation of the draft decision is now awaited and bridging arrangements for the transfer of personal between the wider EEA and the UK will continue until the 30 June 2021 to allow technical confirmation of the draft decision to take place. In the meantime, UK Data Processors, including Local Authorities, can continue to process personal data as if the European GDPR were still effectively in force. Work to establish a Software Asset Management System which will provide a centrally coordinated inventory of all software application used across Council Services commenced in 2020 to establish the extent to which the Council process personal data outwith the UK. To address risks associated with wider international personal data processing appropriate risk assessments will be undertaken in relation to those applications which may present significant risks in the continued

Latest Assessment Due Apr 15, 2021

Latest Assessment 21 April 2021

Next Assessment 15 July 2021

Frequency Every 3 Months

processing of personal data and, if necessary, any viable alternatives to the existing methods of processing. The strengthening of data protection rights has also significantly increased awareness amongst the public, with a resultant increase in volume of subject access requests (SARs), and without an established approach to dealing with these NLC has limited ability to fully understand scale and impact. v) The Council's corporate records stores in Motherwell and Coatbridge hold significant amounts of high-value, irreplaceable, vital records and archives, with permanent or long-term retention periods, often containing personal information or of historic value.	
Risk Description 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 controls which address the additional information security and information governance risks arising from the significant shift to home working triggered by the Covid-19 pandemic. **Due To** Inadequate information security including ICT security systems; Inadequate Information Governance arrangements; Ineffective policies and procedures and audited processes in place; Staff not aware of or adhering to procedures; Ineffective communications with staff; System failure or system is inadequate for required level of protection; Security breach either technical or physical; Unauthorised access to sensitive data; Physical breach either accidental or deliberate; Increase in number of empty council offices with potentially unsecured information and/or systems vulnerable to infiltration, damage or criminal activity; Poor management of confidential information in relation to increase in home working where normal controls may not exist i.e. printing of personal or sensitive data which may be accessible to non-staff and may be unsecured in employee's homes; Lack of confidential waste disposal arrangements; Access to Council ICT facilities (laptops and the data accessible through them) by unauthorised individuals i.e. people living in the same accommodation as an authorised person who is working remotely; Call privacy issues with other household members nearby while on calls/videos; Increase in attempted Cyber Security scams targeting staff during abnormal circumstances when controls may be compromised; Change to cloud based systems and full implications of Digital NL are unknown; lack of service engagement with ICT team, leads to inability to verify compliance with cloud based security principles; competing operational demands impeding progress on management of information risk; lack of key skills and knowledge across the organisation to manage information risk; model of devolved responsibility with no dedicated resource whose sole remit is oversight and progression of information management. Damage to physical records held in the corporate records store by fire, flood, theft, vandalism, pests, environmental conditions and general deterioration of records due to age. **Impact** Extensive adverse media coverage and reputational damage; Breaches of information, resulting in significant fines from e.g. Information Commissioners Office; Legal action and damages; Considerable resources required to remedy any issues and other areas of business negatively impacted by diverted resources being used to address issues; Inability to comply with statutory requests e.g. documentary evidence for court and/or possible legal censure; challenge in dealing with increased volume of SARs within statutory timescales ensuring satisfactory quality of responses. Harm to individuals, especially where Council has duty of care; System availability outages e.g. as we have seen with COVID-19 and not being prepared for initial volume of remote working, loss of vital or historical records, etc.	**Organisation Structure** North Lanarkshire Corporate
Corporate Priorities • Improve North Lanarkshire's resource base	

Inherent Assessment ASM0001859	**Likelihood** - 5	**Impact** - 5	**High** - 25

Likelihood Reason

Increasing instances of successful cyber-attacks on organisations that have controls in place, suggests that an organisation with no controls would be certain to experience security breaches. The significant and fundamental change in the management and delivery of council services means that without appropriate and effective controls, the inherent likelihood of a breach remains high and the nature of how we are using individual's sensitive and personal data, including those vulnerable or shielding, is crucially important not only to avoid a breach but to ensure information is accurate and used efficiently to deliver effective support.

Impact Reason

Inability to use data could foreseeably result in critical services being unavailable, which could significantly impact the health and wellbeing of vulnerable service users. Increasing legislation and regulation in response to data governance failures and 'near misses' e.g. The EU General Data Protection Regulation (GDPR) 2018, and subsequently, the UK GDPR increased the rights of individuals to have more control over aspects of their personal data (e.g. the right to be forgotten, the right to remove data processing consent).

Controls and Actions	**Owner**	**Status**	**Completion Date**
CON0000230 - Data Governance Board (DGB) provides a cross service strategic platform to address information management issues, and ensure lessons learnt from breaches and near misses. terms of reference agreed and subject to annual review - next due 31/03/21	Katrina Hassell	Implemented	9 April 2020
ACT0000379 - CON0000230 - Terms of reference for DGB and DMT agreed and will now be subject to annual reviews.	Katrina Hassell	Complete	31 March 2021
CON0000231 - Data Protection Officer mandatory post ensures compliance with provisions of the DPA 2018 and UK GDPR	Archie Aitken	Implemented	16 December 2020
ACT0000381 - CON0000231 - Development and roll out of SARs process including training	Archie Aitken	Complete	1 January 2020
CON0000232 - Data Management Team (DMT) provides a cross service operational platform to : a. Raise compliance awareness b. Address operational information management issues and focus on ICT Security related compliance c. Establish short life sub-groups to progress specific tasks	Karen MacFarlane	Implemented	16 December 2020
ACT0000109 - CON0000232 - Records Retention schedule being reviewed and to be communicated to staff and published on Connect and website	Fiona Hughes	Complete	31 March 2019
CON0000233 - The Information Governance Policy Framework brings together the Council's information governance policies and ensures that they operate effectively. This includes guidance for staff on the implementation of these policies e.g. Information Classification and Handling Policy, Acceptable Use of ICT Policy as well as guidance on home working and data security.	Karen MacFarlane	Implemented	21 April 2021

ACT0000110 - CON0000233 - Develop and refine KPIs in relation to Information Security & Information Governance and establish reporting. Update 7 October 2020 Suggested KPIs approved by DGB June 2020, procedures to be put in place to start monitor these and report to DGB quarterly.	Karen MacFarlane	Complete	31 May 2020
ACT0000111 - CON0000233 - Information Governance Policy framework review completed, to go to next Policy and Strategy Committee (probably June 2020)	Karen MacFarlane	Complete	30 June 2020
ACT0000539 - CON0000233 - Development and approval of Data Strategy document to help set future strategic direction. Update 7 October 2020 Approved by DGB June 2020 and approved at CMT 29 October 2020	Katrina Hassell	Complete	30 September 2020
ACT0000684 - CON0000233 - Develop a communication that reminds staff about information risks working from home and the council's expectations e.g. no printing of papers: disposal of papers especially confidential papers; use of headsets to enable privacy; locking laptops. Communication to go out at point of relaunch of Interim Home working scheme/Employee Code of Conduct etc.	Katrina Hassell	Complete	31 March 2021
CON0000234 - Laptop and mobile storage device encryption, secure file transfer via Hyve, email encryption. Sophos SWG, Sophos Central AV, control over USB-attached media, email security/scanning, SIEM, patching, network segmentation, assurance reviews (pen tests), firewalls, MFA, remote access controls, etc.	Grant Reid	In Progress	
ACT0000680 - CON0000234 - Further controls to make unauthorised access harder would include requiring stronger Active Directory passwords (only 8 characters at present) and increasing duration currently is 42 days.	Grant Reid	Raised	30 September 2021
ACT0000681 - CON0000234 - Recommended that all relevant staff are provided with a suitable headset to maintain a degree of call privacy. At Jan 2021, 1666 headsets been bought and distributed. Scoping exercise underway to confirm what hardware and peripherals are out there with staff, with a view to developing standard hardware pack which will include appropriate headsets. Review position end March.	Katrina Hassell	Raised	31 March 2021
CON0000235 - Mandatory e-learning courses available for staff in respect of Data Protection Act 2018, Information and Cyber Security Awareness, and Records and Information Management topics. Compliance monitored via DMT and reported 1/4ly via KPIs to Data Governance Board.	Karen MacFarlane	In Progress	
ACT0000112 - CON0000235 - Appointment of specialist Data Protection solicitor within Legal & Democratic Solutions	Archie Aitken	Complete	1 October 2018
ACT0000382 - CON0000235 - Promote uptake of Data Protection Essentials and Data Protection Advanced training modules with Heads of Service including campaign to raise awareness of Learn NL, encouraging registration and Managers to view, and monitor uptake via the dashboards therein. TOD to assist with full review of training framework/matrix including check uptake of mandatory e-learning, development of new model of training for TOD to deliver with technical input including training required for roll out of Office 365.	Karen MacFarlane	Raised	31 August 2021

ACT0000679 - CON0000235 - Ensure information security risks associated with home working, and council's expectations of staff are reflected in mandatory training. Review of training due.	Pauline McCafferty	Complete	31 March 2021
CON0000236 - Council's DPO also engaged as DPO to many ALEOs, providing assurance regarding ALEO information governance arrangements.	Paul Corrigan	Implemented	16 December 2020
ACT0000115 - CON0000236 - ALEOS Data Protection Workshop (where Head of Legal Services Appointed as Data Protection Officer) Need to check if this action is completed or not being progressed.	Paul Corrigan	Complete	31 October 2018
CON0000237 - The Records Manager acts as a consultant on all records and information compliance matters.	Fiona Hughes	Implemented	7 August 2019
ACT0000114 - CON0000237 - Maintain Cyber Essentials (Changed from Cyber Essentials Plus as per instructions Karen MacFarlane 7 Aug 2019)	Karen MacFarlane	Complete	31 July 2019
CON0000238 - Records Management Plan is in place	Fiona Hughes	Implemented	16 December 2020
CON0000239 - Information Asset Register covers all mediums, and identifies information asset owners and administrators, and this is regularly reviewed - only access not content, to be controlled and monitored via DMT.	Karen MacFarlane	In Progress	
ACT0000380 - CON0000239 - Initial review of IAR complete, continual review and monitoring with move to new platform underway.	Karen MacFarlane	Underway	31 July 2021
CON0000240 - Records retention schedule gives clear guidance to staff on the management and disposal of all formats of information	Fiona Hughes	Implemented	9 May 2019
CON0000241 - Collaboration and communication tools for use on collaborative work and projects across services maintains confidentiality and security to small groups including deployment of new digital packages such as Microsoft Teams.	Karen MacFarlane	In Progress	
ACT0000682 - CON0000241 - Completion of deployment of new digital packages including New Microsoft Teams/O365 across the organisation.	Grant Reid	Raised	30 April 2021
CON0000242 - Confidential waste paper securely stored, removed and disposed of under the corporate shredding contract	Karen MacFarlane	In Progress	
ACT0000481 - CON0000242 - Review contractual options and requirements, as well as procurement process for corporate shredding.	Karen MacFarlane	Raised	30 September 2021
CON0000243 - Twice yearly review of accounts with elevated privileges.	Grant Reid	Implemented	9 May 2019

CON0000244 - Data quality checks by Data Custodian deals with management of information across systems.	Karen MacFarlane	Implemented	9 May 2019
CON0000636 - Specialist Data Protection solicitors (2 of) within Legal & Democratic Solutions	Paul Corrigan	Implemented	9 May 2019
CON0000637 - Information Risk Manager acts as an internal consultant for all information security compliance matters	ROB LEITCH	Implemented	9 May 2019
CON0000735 - Corporate SARS recording and reporting process.	Paul Corrigan	Planned	
ACT0000476 - CON0000735 - Consider options and associated technical solutions for managing the wide variety of information risks (AIR, FOI, SARS, Complaints) within the digital transformation operating model. Agreed on backlog for development.	Katrina Hassell	Raised	30 June 2021
ACT0000482 - CON0000735 - Consider scope to fully deploy a corporate redaction tool to improve quality of responses. Licensing and costs under consideration by each service. For consideration as part of wider review of SARs process/arrangements.	Paul Corrigan	Underway	30 June 2021
CON0000848 - Enterprise Architecture Governance Group.	Katrina Hassell	Implemented	31 July 2019
CON0000849 - PSN Compliance	Grant Reid	Implemented	3 February 2020
CON0001359 - Progress cloud-hosted EDRMS rollout in line with Office 365 and Digital NL programme	Karen MacFarlane	Planned	
ACT0000113 - CON0001359 - Progress cloud-hosted EDRMS rollout in line with Office 365 and Digital NL programme	Karen MacFarlane	Raised	31 January 2022
CON0001383 - Corporate and Service Business Continuity Plans in place and stress tested to inform priorities and decision making	Andrew McPherson	Implemented	5 February 2021
CON0001384 - 3rd party processing agreements been put in place with some partners and providers.	Careen Hendry	Implemented	5 February 2021
CON0001385 - Data Sharing Agreements in place with partners such as NHS regarding shielding individuals etc.	Careen Hendry	Implemented	5 February 2021
CON0001386 - Secured Premises with secure storage and monitoring of security arrangements.	Chris Sullivan	Implemented	21 April 2021
ACT0000683 - CON0001386 - Prompt Heads of Service to ensure that in relation to vacated locations, they are satisfied that all key information/files/systems especially sensitive data which may have been left unsecured when premises were suddenly vacated is known, and appropriately protected, secured and monitored where possible i.e. for water leaks, damage etc - 21-4 E Munro confirmed this is happening and is ongoing via their team on behalf of Chris.	Chris Sullivan	Complete	28 February 2021

CON0001477 - To preserve records contained within it, the Corporate Records Stores have 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.			Fiona Hughes	In Progress	
ACT0000731 - CON0001477 - Implementation of similar risk controls where feasible at second records store to that in place at the Heritage Centre (may be restrictions on what is possible).			Fiona Hughes	Underway	31 August 2021
Residual Assessment ASM0001859	**Likelihood** - 5	**Impact** - 4		**High** - 20	

Likelihood Reason

Frameworks, policies, and associated training are in place, but require review and more effective communication mechanisms to ensure working practices remain embedded. Significant amounts of Council information is still held in paper format and this is one of the mediums most at risk of loss. The scoring recognises that some of the actions proposed pre covid will have matured and would likely have resulted in an improved risk, with the application of Covid it may be reasonable to suggest that the risk is back at original 20 scoring, recognising the additional mitigations already put in place, but also ongoing actions which will require to be completed.

Impact Reason

The Scottish Government Cyber Resilience review will set a new standard for all public bodies. It is as yet unclear how the Council's current arrangements compare with these recently developed expectations, however the group recognises there is a question mark over the adequacy and effectiveness of much of the current controls.