North Lanarkshire Council
Report

Audit and Scrutiny Panel

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

ICT Operational Capability Risk - Deep Dive

From Head of Business Solutions

E-mail HassellK@northlan.gov.uk **Telephone** 07903 096 121

Executive Summary

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

This report focusses on the deep dive of the ICT Operational Capability risk due for assessment as of September 2021. With details having now been reviewed and signed off by the Enterprise Architecture Governance Group (EAGG) members on 3 November 2021, this report provides panel members with an update on measures to address this risk, which carries a high residual score. The report provides an overview of existing controls and actions taken to date to mitigate against this risk, as well as further actions planned to continue to manage and update this risk to fully reflect the changing landscape of ICT service delivery.

Recommendations

The Panel is invited to:

1. note the actions taken to date to manage the ICT Operational Capability Risk
2. note the on-going actions to manage this risk as detailed in paragraphs 2.6 to 2.10
3. note the planned actions detailed in paragraphs 2.11 to 2.14.

The Plan for North Lanarkshire

Priority	All priorities
Ambition statement	All ambition statements

1. Background

1.1 The Council increasingly relies heavily on ICT solutions and infrastructure to support it in the delivery of its services. Covid response exacerbated this, requiring services to adapt and change at a more aggressive rate than envisaged within the Council's DigitalNL transformation programme. The shift to home working, whilst technically accommodated at pace by Business Solutions, has brought additional demands, challenges, and support requirements.

1.2 The demands of the digital transformation programme although a known requirement, continue to place pressures on operational capability, particularly as the programme transitions from the build to migrate cycle. The financial commitments to the programme and the dedicated partner resource place timeline restrictions on our in-house resources, with limited flexibility.

1.3 The Council has a very lean level of ICT resource available[1] to deliver its strategic priorities and ambitions and maintain satisfactory support for Business as Usual (BAU) services. Support levels within Business Solutions (including Wipro and short-term fixed contracts) see 98.22 FTE supporting the rapidly changing infrastructure and security requirements of 15,622 FTE. Within these totals, only circa. 27 FTE are available to support the development, implementation and maintenance of the technological portfolio presently used by 9,471 FTE. Panel members may wish to note these 27 FTE support the software requirements of all service areas excluding Education, which presently has additional dedicated technical support equivalent to circa. 40 FTE.

1.4 Our ICT teams, already stretched in delivering on the above requirements, are also faced with supporting and progressing an increasing technological portfolio (due in part to the transformation programme, as both existing and new solutions have significant transition overlap), and accelerated rate of change from 3rd party suppliers looking themselves to introduce more Software as a Service (SaaS) products. Striking this balance is progressively challenging.

1.5 The known estate rationalisation, but unknown timelines, creates uncertainty in support and procurement areas, requiring compromise positions being adopted, which reduces opportunity for efficiency.

1.6 Due to the terms and format of the Systems Integrator (SI) contract, it is currently challenging for Business Solutions staff to be immersed in the production and support side of the new suite of solutions, particularly within the Digital Platform workstream, and to date, this has resulted in the council relying upon the SI – who already have a significant workplan – to deliver additional developmental opportunities.

1.7 The Council, like all large organisations, continues to be targeted by cyber-attacks aiming to disrupt service delivery, and our increasing use of digital cloud and mobile services expands our visible attack surface to 3rd party actors. This requires additional vigilance and monitoring, requiring that we deploy resources to mitigate/build resilience against them, responding appropriately to incidents, to maintain service delivery and business continuity.

1.8 Furthermore, the Scottish Government currently seeks assurance from Scottish Public Bodies of consistent level of accreditable controls, with failure to provide this assurance having the potential to result in additional scrutiny and in some areas financial penalty.

---

[1] *% of ICT FTE to Council FTE: full council = 0.88%; Education only = 0.65%; All services excluding Education and recognising outsourced Wipro resource = 1.03%. Details obtained through SOCITM membership indicates an ICT support average of 1.25% for other local authority members, but such does vary depending on levels of outsourcing in operation.*

1.9 It is generally recognised that low numbers of students undertaking ICT-related courses is resulting in a shortage of ICT skills within the marketplace in Scotland at a time when these skills are becoming more sought after as all businesses adapt to new working practices. This is envisaged to continue, with the skills shortage recently demonstrated as a contributory factor with several failures to award contracts following candidate recruitment. Predominantly this can be attributed to scarcity of resources nationally though the financial packages which the Council can offer versus those of private sector competitors cannot be ignored. The Council will therefore continue to face challenges in terms of recruiting skilled staff moving forward.

1.10 The Councils service delivery partner Wipro has similar challenges, but additionally the construction and inflexibility of the existing contract terms creates additional challenges to accommodating the required rate of change now seen in the authority.

1.11 In short, the previously known demands and our stretched capacity to deal with, is currently further stretched due to Covid response, Organisational change, and the associated digital programmes, with all thus giving rise to a high level of risk in respect of ICT Operational Capability.

---

2. Report

2.1 The council identifies and monitors significant risk to its operations. The ICT Operational Capability 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 16 (likelihood and impact both reducing to 4). This residual rating results in the risk being assessed quarterly. This assessment of 16 remains unchanged from the quarterly review completed in June 2021 and reported to the Corporate Management Team (CMT) in July.

2.2 The Panel are aware that the agreed approach to the management of 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 Enterprise Architecture Governance Group (EAGG) with the Head of Business Solutions identified as the Corporate Risk Lead. This risk was most recently reviewed by EAGG members on 3 November 2021, with all feedback appropriately incorporated into the deep dive attached as Appendix one.

2.3 The risk is that ICT Operations may not have the capacity/capability to support the Council and its partners in delivering Services, meeting Strategic Objectives, ensuring secure operations, and facilitating change.

2.4 The list of factors that contribute towards this risk can be long. The following is a high-level summary of the principal <u>generic</u> factors that influence this risk across all industries:

- Covid accelerated the need for remote working, and although our enterprise infrastructure is moving in the right direction, we are between the 'old world' and the 'new world' so still need to address a range of technologies which are not currently fit for purpose.
- The Business Solutions employee structure now reflects the requirements of a modern digital council (our new world), but the legacy of a traditional ICT estate and associated processes (the old world) must still be managed on an ongoing basis.
- Service expectations regarding maintenance and support for current bespoke in-house business applications such as HSMS, mySWIS etc.
- Need to upskill current resources particularly given challenges experienced on occasion in respect of attracting external candidates to our remuneration package.
- Generalised resource pool with external contractors with no specificity training in place (e.g., External contractor will have O365 skills but does not necessarily know how NLC have customised their O365 set up).
- Lack of workflow process for use with internal ICT governance and standards (i.e., acceptable use of ICT, procurement, security).
- Requirement to update several policies and strategies which support ICT operations.

2.5 The impacts of having an insufficient level of ICT operations available are likely to be significant, and may include:

- Non-achievement or reduced delivery of corporate and service priorities, including the DigitalNL programme and its associated savings
- Errors or corruption arising from unplanned system changes
- Internal or external data loss from malicious hackers
- Increased security incidents
- Loss of and/or inability to access key systems and data
- Significant reputational damage for NLC and/or partner organisations
- Increased failure rates from ageing technologies
- Sanctions/fines from schemes and regulators for non-compliance
- Disconnection from regulated essential services
- Efficiencies in terms of cost and service delivery not being exploited or fully maximised

2.6 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:

- Technical Design Authority (TDA), Enterprise Architecture Governance Group (EAGG) and Data Governance Board (DGB) are all in place and enable oversight of this risk and associated controls and actions including review of skills and resources required.
- Digital & ICT Strategy approved, in place and updated on an ongoing basis.
- Well established procurement processes enable robust selection of ICT partners.
- Ongoing review and update of the ICT Disaster Recovery and Business Continuity plans plus bi-annual testing.

- Robust network design including firewalls, antivirus & antimalware systems and two factor authentications to control unauthorised access.
- Use of automatic detective and preventative technologies (in respect of security incidents and inappropriate access and damage to council information)
- ICT Code of Connection controls external access to ICT resource.
- Information Governance Framework
- Dedicated resource within ICT Focussing on Programme, Change and Security Management
- Corporate Project Management methodology approach augmented by local project management approaches for specialist areas ensures consistency.
- Service management system is in place
- ICT operational procedures and guidance, including operations manual and solutions guide for each application.
- Availability of additional specialist/ resources through Digital Business (DBP) and System Integrator (SIP) framework and partnerships
- Fully revised and aligned Business Solutions structure, with functions identified as key through DBP and SIP arrangements.
- Technical library for all solutions documentation.
- Staff IT security awareness training modules

2.7 The council is no exception to the rule that organisations must continue to develop their capability posture to address the ongoing changing environment. Activities are on-going to maintain and enhance the council's operational capability and these range from technical to process, procedural and staff awareness raising. Appendix one demonstrates this is actively being pursued through for example actions ACT0000598, ACT0000599 and ACT0000600.

2.8 In terms of governance, the Technical Design Authority (TDA) provides a forum to look at technical solutions and how they fit with the council's technical standards and principles. The Enterprise Architecture Governance Group (EAGG) considers holistically how proposed solutions comply with organisational and architectural principles e.g., do they represent good value, and do we understand how we will use them and provide support

2.9 Supporting the work of the TDA and EAGG the council has implemented a variety of policies and procedures including the Information Governance Framework and the ICT Code of Connection. These undergo regular review and include guidance for staff on the implementation of relevant policies. As outlined within Appendix one (CON0000227), the council has appointed an Operational & Support Manager responsible for the delivery of the key areas of ICT operations supporting the business-as-usual operation of the council's ICT infrastructure. The council has also appointed a Programme manager who is responsible for the management and delivery of all projects and programmes within the Business Solutions function

2.10 Technical activity that is on-going to improve efficiency and ease pressure on ICT operations includes M365 migration, exchange migration, Dev-Ops live, 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.

2.11 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 also planned following full roll out of M365. Appendix one demonstrates these mitigations are actively being pursued through actions ACT0000696, ACT0000739 and ACT0000740.

2.12 Future technical and administrative/procedural initiatives and solutions will always be required to be built on what has already been established. Our planned activity to further mitigate exposure to this risk includes finalising knowledge transfer/handover arrangements with Agilisys, 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.

2.13 In recognising the Council has a very lean level of ICT resource available, ACT0000741 outlined within Appendix one is presently a key area of focus for Business Solutions with significant change and developments underway. The Panel will be aware that the Transformation and Digitisation Committee of 17 November approved the recommendation to insource services presently delivered by our Wipro service delivery partner effective from April 2022.

2.14 To fulfil the requirement to deliver an independent and integrated ICT service capable of supporting council services and all nine community boards outlined within the Delivering for Communities report (Policy and Strategy Committee, December 2020), a dedicated Business Solutions Structure Working Group has responsibility for shaping future delivery options. This group includes Trade Union representatives from Unison, GMB and Unite, as well as representatives from Business Solutions, People and Organisational Development, Community Learning & Development and Education & Families. This group is presently exploring opportunities to improve capacity which may arise from the transfer of the Education technician support service and the insourcing and harmonisation of Culture and Leisure North Lanarkshire resources.

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 Regulation

4. Impact

4.1 Financial impact

Effective operational capability management can assist in ensuring the council does not incur fines 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.

4.2 HR policy / Legislative impact

Delivery of effective operational capability requires ongoing knowledge of all associated employee relations policies. In addition, partnership working remains ongoing with trade union representatives through the dedicated Business Solutions Structure Working Group.

4.3 Technology / Digital impact

Technology / digital impacts will be significant 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). All proposals, and the oversight of this corporate risk, are routinely considered through the Enterprise Architecture Governance Group (EAGG), with this deep dive most recently approved by the Group on 3 November 2021.

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 does 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

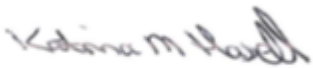
If the council does not effectively address this risk then there are considerable risks to the council in terms of reputational damage, loss of service (and significant costs to restore service), loss of confidence amongst staff and stakeholders and the possibility of very significant fines should we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

5. Measures of success

5.1 The continued effective management of this risk with 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 1** – ICT Operational Capability Risk Deep Dive Report



Katrina Hassell
Head of Business Solutions

Appendix 1 – ICT Operational Capability Risk Deep Dive Report

Deep Dive Report RIS0000018	**Risk Title** ICT Operational Capability	**Owner** Katrina Hassell
Risk Context NLC increasingly relies heavily on ICT solutions and infrastructure to support the organisation in the delivery of its services. Covid response has exacerbated this, requiring services to adapt and change at a more aggressive rate. The shift to home working, whilst technically accommodated through the 'corporate' Business Solutions teams, has brought additional demands, challenges, and support requirements. The demands of the digital transformation programme whilst a known requirement, continue to place pressures on the operational capability of the 'corporate' ICT resource, particularly as the programme transitions from the build to migrate cycle. The financial commitments to the programme and the dedicated partner resource place timeline restrictions on the service, with little flexibility. The recognised lean levels of ICT resources (98.22 FTE – including Wipro – to support the infrastructure and security requirements of 16,973 FTE) available are not only stretched with the above, but Business As Usual demands (BAU), an increasing technological portfolio (due in part to the transformation programme, as both existing and new solutions have significant transition overlap), and the rate of change from 3rd party suppliers as more Software as a Service (SaaS) products are introduced result in the delivery of strategic priorities and ambitions and maintenance of satisfactory support for BAU services being progressively challenging. The known estate rationalisation, but unknown timelines, creates uncertainty in support and procurement areas, requiring compromise positions being adopted, which reduces opportunity for efficiency. Due to the format of the Solutions/System Integrator (SI) contract it continues to be challenging to get Business Solutions staff involved in the production and support side of this new suite of solutions, particularly within the Digital Platform workstream, which has a direct result of the council relying upon the SI for additional developmental opportunities. NLC, like all large organisations, continues to be targeted by cyber-attacks aiming to disrupt service delivery, and our increasing use of digital cloud and mobile services expands our visible attack surface to 3rd party actors. This requires additional vigilance and monitoring, requiring that we deploy resources to mitigate/build resilience against them, responding appropriately to incidents, to maintain service delivery and business continuity. Furthermore, the Scottish Government currently seeks assurance from Scottish Public Bodies of consistent level of accreditable controls, with failure to provide this assurance having the potential to result in additional scrutiny and in some areas financial penalty. It is generally recognised that low numbers of students undertaking ICT-related courses is resulting in a shortage of ICT skills within the marketplace in Scotland at a time when these skills are becoming more sought after as all businesses adapt to new working practices. This is envisaged to continue and has been demonstrated with several failures to award following recruitment. Whilst this can predominantly be attributed to scarcity of resources nationally, the financial packages the Council can offer are a factor with it therefore envisaged that challenges in terms of recruiting skilled staff moving forward will continue. The Councils service delivery partner Wipro has similar challenges, but additionally the construction and inflexibility of the contract creates additional challenges to accommodating the required rate of change now seen in the authority. In short, the previously known demands and our stretched capacity to deal with, is currently further stretched due to Covid response, Organisational change, and the associated digital programmes, thus the risk against Operational Capability to delivery remains high.	**Latest Assessment Due** Sept 4, 2021 **Latest Assessment** Nov 3, 2021

Risk Description	**Organisation Structure**
ICT Operations may not have the capacity/capability to support the Council and its partners in delivering Services, meeting Strategic Objectives, ensuring secure operations, and facilitating change. **Due To** ICT currently sits between 'old world' and 'new world' therefore whilst enterprise infrastructure is moving in the right direction it is still not currently fit for purpose for the modern world. The 'corporate' ICT employee structure transitioning between old world and new world, with roles and responsibilities not yet fully embedded whilst staff continue to support legacy products. Service expectations regarding maintenance and support for current in-house business applications (e.g., HSMS, mySWIS). Need to upskill current resources as it proves challenging on occasion attracting external candidates to NLC package. Generalised resource pool with external contractors with no specificity training in place (e.g., External contractor will have O365 skills but does not necessarily know how NLC have customised their O365 set up). Lack of scalable workflow process for use with internal ICT governance and standards (i.e., acceptable use of ICT, procurement, security). Insufficient contract management practices. Inadequate or out of date policies and strategies to support operations. **Impact** Non-achievement or reduced delivery of corporate and service priorities, including the DigitalNL programme; Errors or corruption arising from unplanned system changes; Internal or external data loss from malicious hackers; Increased security incidents; Loss of and/or inability to access key systems and data; Significant reputational damage for NLC and/or partner organisations; Increased failure rates from ageing technologies; Sanctions/fines from schemes and regulators for non-compliance; disconnection from regulated essential services; Efficiencies in terms of cost and service delivery not being exploited or fully maximised.	North Lanarkshire Corporate

Corporate Priorities

- Improve economic opportunities and outcomes
- Support all children and young people to realise their full potential
- Improve North Lanarkshire's resource base
- Enhance participation, capacity, and empowerment across our communities
- Improve the health and wellbeing of our communities

Inherent Assessment ASM0002109	**Likelihood -** 5	**Impact -** 5	**High -** 25

Likelihood Reason

The continued use of current BAU solutions whilst transitioning to new solutions will result in more not less systems to manage. Increasing frequency of cyber-attacks coupled with the rate of change the organisation will experience, will result in new and increasing cyber risks.

Impact Reason

Some services will be unable to function to full effect without IT Solutions in place. Supportability of in-house applications (e.g., HSMS, mySWIS) reduces to reflect either reductions or a reallocation of development resources. The council's strategic direction in this regard is now agreed, however lack of capacity/numbers/skills within the 'corporate' pool continues to carry a risk of the Digital NL programme and current BAU creating a competing demand for ICT support resources

Controls and Actions	**Owner**	**Status**	**Completion Date**
CON0000219 - Technical Design Authority, Enterprise Architecture Governance Group, and IGWG (now the Data Governance Board) in place and enable oversight of this risk and associated controls and actions including review of skills and resources required.	Katrina Hassell	Implemented	19 December 2019
ACT0000107 - CON0000219 - Technical Design Authority/Enterprise Architecture Governance Board in place however membership and TOR need reviewed to ensure effectiveness	Katrina Hassell	Complete	31 December 2018
ACT0000386 - CON0000219 - Review IGWG, IMWG membership and terms of reference.	Grant Reid	Complete	31 March 2019
CON0000220 - Digital & ICT Strategy approved Sept 2019	Katrina Hassell	Implemented	21 June 2021

ACT0000099 - CON0000220 - Review ICT Policies and Strategy and guidelines to identify suitability, effectiveness and gaps following finalisation of the design phase of DigitalNL. Interim review of policies approved by Policy & Strategy Committee June 2020, full review to be complete by end March 2021.	Grant Reid	Complete	31 March 2021
ACT0000106 - CON0000220 - Introduce Strategic ICT training plan (aligned to technology strategy/Digital NL aspirations), training programme and skill matrix to ensure effective deployment of DigitalNL technologies and in line with new Business Solutions organisational structure. Skills analysis and training plan complete but will be subject to continual review.	Katrina Hassell	Complete	31 August 2020
CON0000221 - Well established procurement processes enable robust selection of ICT partners	James McKinstry	Implemented	19 December 2019
CON0000222 - Ongoing review and update of ICT DR & Service BC Plans plus bi-annual testing.	Grant Reid	Implemented	13 January 2021
ACT0000104 - CON0000222 - Review and update of current ICT Disaster Recovery. Review completed, further actions to be added for testing of plan on a phased basis commencing November 2020.	Rob Leitch	Complete	30 September 2020
ACT0000105 - CON0000222 - Review and update of Service Business Continuity Plans (thereafter annual testing)	Aileen McMann	Complete	30 June 2018
CON0000223 - Robust network design including firewalls, antivirus & antimalware systems and 2FA to control unauthorised access.	Grant Reid	Implemented	27 January 2020
ACT0000102 - CON0000223 - Completion of tasks associated with network redesign. (as at Jan 2020 have taken as far as possible this will now be superseded by DigitalNL.	Grant Reid	Complete	1 January 2019
CON0000224 - Use of automatic detective and preventative technologies (in respect of security incidents and inappropriate access and damage to council information)	Grant Reid	Implemented	21 May 2020
ACT0000103 - CON0000224 - Further development of SIEM to enhance controls.	Grant Reid	Complete	30 June 2020

CON0000225 - ICT Code of Connection controls external access to ICT resource	Rob Leitch	Implemented	16 December 2019
CON0000226 - Information Governance Framework	Karen MacFarlane	Implemented	27 January 2020
CON0000227 - Dedicated resource within ICT focussing on Programme, Change and Security management	Grant Reid	Enhancing	27 January 2020
ACT0000696 - CON0000227 - Actively manage internal resources to ensure we are maintaining and improving our skill base. Annual review.	Grant Reid	Underway	31 December 2021
ACT0000739 - CON0000227 - Implement a mechanism to effectively manage resources on an ongoing basis across the ICT function.	Grant Reid	Underway	31 December 2021
CON0000228 - Corporate Project Management Methodology approach augmented by local PM approaches for specialist areas ensures consistency.	Katrina Hassell	Implemented	16 December 2019
CON0000229 - Service Management System in place	Grant Reid	Implemented	10 May 2019
CON0000639 - ICT operational procedures and guidance, including operations manual and solutions guide for each application.	Grant Reid	Enhancing	19 December 2019
ACT0000740 - CON0000639 - Audit process to be implemented to ensure operational procedures and guidance (inc. operations manual and solutions guide) are in place for each application.	Grant Reid	Raised	31 March 2022
CON0001037 - Availability of additional specialists/resources through Digital Business (DBP) and System Integrator (SIP) partnerships	Katrina Hassell	Implemented	4 February 2020
CON0001038 - Fully revised and aligned corporate Business Solutions structure, with functions identified as key through DBP and SIP arrangements.	Katrina Hassell	In Progress	

ACT0000598 - CON0001038 - Fully implement Phase one of revised Business Solutions structure, developing functions identified as key through DBP and SIP arrangements. Significant progress made but completion delayed due to job evaluation process.	Katrina Hassell	Underway	31 March 2022
ACT0000741 - CON0001038 - Implement process to ensure structure of ICT function continues to stay relevant to the wider organisational needs, and previous approvals (e.g.: Integrated ICT support model, Delivering for Communities etc)	Katrina Hassell	Underway	31 March 2022
CON0001039 - Technical library for all solution documentation.	Grant Reid	Implemented	30 September 2020
ACT0000599 - CON0001039 - Develop a technical library for all solution documentation.	Grant Reid	Complete	30 September 2020
CON0001040 - Staff IT security awareness training modules	Grant Reid	Implemented	23 February 2021
ACT0000600 - CON0001040 - Work with TOD to develop staff IT security awareness training modules - New ICT Security Module launched.	Grant Reid	Complete	30 June 2020

Residual Assessment ASM0002109	**Likelihood -** 4	**Impact -** 4	**High -** 16

Likelihood Reason

Continual shift by Services to an IT enabled requirement for customer service delivery has resulted in substantial growth in the product set utilised by the Council. This coupled with previous reduction in IT staffing levels has resulted in internal resource skill levels being severely diluted, with limited capacity for the high levels of specialism that the organisation now needs. The Service was successful in getting approval for 4 additional posts within Infrastructure, 2 fixed term and 2 permanent posts, and has been able to fill several of its vacancies over the past 3-6 months. Although the Council has additional capacity through its specialist partnership arrangements with Agilisys and PWC, the competing demands arising between BAU support and digital transformation will continue in the short to medium term as both environments require to be resourced. This coupled with the introduction of new solutions and products to the user base, results in a significant rise in the Incident, Change and Requests seen via the service desk. The transition to homeworking although accommodated, has not been without its challenges and this will continue to be the case as more council services look to redesign and recover. This results in a continual rise in service desk calls handled by our delivery partner Wipro, who do not have planned capacity to deal with these increased volumes. The controls currently in place around governance, policies and procedures have all improved and with appropriate training and knowledge transfer/upskilling being progressed with Agilisys, will bring further improvements, (however this represents another short to medium term draw on our corporate resource pool). As transition to phase one of our revised structure

completes, this will realise organisational benefits over the coming year. However, insourcing of CLNL and the subsequent alignment to Council standards represents a significant body of work. Recent relaxation of covid restrictions may also result in increased demand as services potentially looks to adjust operational working practices. Lastly as the Digital Workplace transition support is mostly complete, with NLC now having exited the Cloud Service Partner agreement with Agilisys (June 2021) to self-manage Azure and presently planning the exit management arrangements of Agilisys in the Digital Platform area, the Council will gain further understanding of the Business-as-Usual effort associated within maintaining these new environments. Taking all factors into an overall consideration, in the short to medium term the likelihood/proximity of this risk continues to remain at level 4.

Impact Reason

ICT Disaster Recovery has also suffered due to pressure of maintaining services to required standards with a very lean team. In the event of a loss of the Motherwell data centre, there is currently no capacity to operate the level of services that would be expected in a timely manner. The successful move of the Councils main DR site from Caird to Datavita and the focus on informed assessment of Azure DR options for all systems going forward, overseen by the EAGG, will now reduce the impact of this risk from its previous levels. However, this will take time as systems transition and/or are replaced. With regards to the constant threat of Cyber-attacks, it is normal for all organisations to be attacked daily, which is the case for NLC, but current controls have so far mitigated against the impact. There is always the possibility that future attacks will be of a more sophisticated nature and could indeed cause major disruption. The Council is working on introducing additional security solutions to enhance the controls in place, but available funding constrains the pace and capacity to improve skill sets. Taking all factors into an overall impacts consideration, the residual rating of this risk remains at level 4 (major).