Report to:	**AUDIT COMMITTEE**
Relevant Officer:	Steve Thompson, Director of Resources Tony Doyle, Head of ICT Services Mark Towers, Director of Governance and Partnerships Neil Jack, Chief Executive
Meeting	15 June 2023

STRATEGIC RISK REGISTER DEEP DIVE – TECHNOLOGY

1.0 Purpose of the report:

1.1 To consider a progress report on individual risks identified in the Council's Strategic Risk Register.

2.0 Recommendation(s):

2.1 To consider the controls being implemented to manage the strategic risk relating to technology.

3.0 Reasons for recommendation(s):

3.1 To enable the Corporate Leadership Team (CLT) and Audit Committee to consider an update and progress report in relation to an individual risk identified on the Strategic Risk Register.

3.2	Is the recommendation contrary to a plan or strategy adopted or approved by the Council?	No
3.3	Is the recommendation in accordance with the Council's approved budget?	Yes

4.0 Other alternative options to be considered:

4.1 N/a

5.0 Council priority:

5.1 The risk impacts on all of the Council's priorities.

6.0 Background information

6.1 At its meeting in March 2023, the Audit Committee agreed to continue to invite Strategic Risk Owners to attend future meetings to provide updates and progress reports in relation to the individual risks identified on the Strategic Risk Register.

6.2 Does the information submitted include any exempt information? No

7.0 List of Appendices:

7.1 Appendix 3(a) - Strategic Risk Register Deep Dive – Technology

8.0 Financial considerations:

8.1 The controls being implemented will be done so within current budget constraints.

9.0 Legal considerations:

9.1 Risks need to be effectively managed in order to comply with relevant legislation.

10.0 Risk management considerations:

10.1 To enable CLT and Audit Committee to gain assurance that strategic risks are being effectively managed.

11.0 Equalities considerations:

11.1 Equality analysis should have been undertaken, where necessary, when decisions were made in relation to the identification of the actions identified in this document. As this report presents monitoring against pre-agreed actions, no further equality analysis has been undertaken as part of this report.

12.0 Sustainability, climate change and environmental considerations:

12.1 Sustainability, climate change and environmental matters should have been considered, where necessary, when decisions were made in relation to the identification of the actions identified in this document. As this report presents monitoring against pre-agreed actions, no further analysis has been undertaken as part of this report.

13.0 Internal/external consultation undertaken:

13.1 The progress report has been prepared in conjunction with risk owners.

14.0 Background papers:

14.1 N/a

Appendix 3(a): Risk Category: Technology

Risk Appetite: Cautious

Risk: a) Cyber Threats

Risk Owner: Director of Resources

Gross Risk Score	25	Impact – 5	Likelihood – 5

What impact does this have?

- Cyber fraud.
- Reputational Damage.
- Loss of compliance with security regimes.
- Loss of confidence in using Council online services.
- Monetary penalties / fines.

What opportunities does this create?

- Improved knowledge and awareness across departments on identifying phishing emails and other cyber threats.
- Participate in training and knowledge gathering opportunities.
- Robust cyber security controls in place.

What controls do we already have in place?

- Investment in Sandbox technology.
- SIEM (Security Information Event Management) implemented to proactively monitor activity on the network.
- The use of blacklists / reputation to authenticate emails received and artificial intelligence being used to further detect and reduce the amount of SPAM e-mails.
- Proactive engagement with regional and national cyber security agencies.
- ICT Security Policy in place supported by mandatory Cyber Awareness Training.
- Two internet connections maintained to provide resilience.
- Cyber policy in place with reputable insurer providing breach response and liability cover.
- Full Sender Policy Framework (SPF) checking in place and adherence to the National Cyber Security Centre (NCSC) guidelines for Securing Government email.
- White listing utilised to mitigate the risk of being hijacked.

Net Risk Score	20	Impact – 5	Likelihood – 4

What are we doing to further manage the risk?

Continue to develop and refine technologies to provide proactive alerting and monitoring of the changing threats.

The ICT Team continue to develop proactive monitoring tools which indicate unusual activity and investigate alerts from these tools. As the tools used continue to embed they become more intelligent

which also helps reduce the risk of a cyber-attack.

The Head of ICT is liaising with the National Protective Security Authority about the potential of implementing a phishing tool which could be deployed at the Council, dependent on its benefits and its ability to support the proactive approach to cyber risk mitigation.

Two external organisations have attempted on separate occasions to gain physical access to the main data centre and failed on both occasions as part of testing arrangements.

Should an incident occur, cyber insurance is in place with a new insurer being appointed for the current financial year. As part of this service regular testing is undertaken by the insurer which provides an additional level of checking around the robustness of the Council's controls.

Ensure all employees are using two factor authentication on all key systems.

All key systems hosted in the cloud such as the new HR and Payroll system, the new finance system and Microsoft 365 have two factor authentication in place. The ICT service are continuing to develop two factor authentication across all privileged access accounts including some on-premises systems.

Risk for other systems are being considered and will be addressed accordingly.

The ICT team are currently implementing a process which enables self-service password resets and this presents an opportunity to strengthen password policies, enforcing password policies and introducing a password dictionary. This will also create efficiencies on the ICT Helpdesk who will be better able to focus their resource on other issues rather than resetting passwords.

Undertake a cyber-incident exercise to gain assurance that the disaster recovery protocols in place are fit for purpose.

Discussions are currently taking place with Lancaster University about the development and facilitation of such an exercise which is scheduled to take place in September 2023.

Target Risk Score	15	Impact – 5	Likelihood – 3

What will these additional actions achieve?
The Council's approach to cyber security is to focus on proactive early warning which helps reduce the potential of a cyber-attack and also reduces the response time should an attack occur. The actions being taken in the current financial year will also reduce the risk of compromised passwords, provide ongoing mitigation against key risk areas, such as ransomware or phishing attacks, and reduce the risk of high value accounts being compromised.

What barriers do we face?
The evolution of attacks in terms of level of sophistication coupled with an increased number of attacks due to geo-political tensions make cyber security an ongoing challenge.

Do these actions contribute to the sustainability of the Council?
The increased dependency by Council services on the ability to access and use IT. Therefore, any

unplanned downtime due to an attack could have a significant impact on the Council being able to sustain an appropriate level of service delivery.

Do these actions impact on the Council's finances?
A successful cyber-attack could have a significant financial impact over and above not being able to deliver key Council systems and the associated reputational damage. There is a risk of fines should any data be stolen which could be very significant due to the regulatory frameworks in place.

How does this contribute to the Council Plan?
Access to secure IT is a key factor in organisational resilience.

Any links to other strategic risks?
Information and Legal

Any additional changes to this strategic risk?
A significant growth area is in relation to artificial intelligence which brings its own emerging set of risks should artificial intelligence be used in the future to carry out cyber-attacks.

Risk: b) Non-compliance with data protection legislation.

Risk Owner: Chief Executive, Director of Governance and Partnerships, Director of Resources

Gross Risk Score	20	Impact – 4	Likelihood – 5

What impact does this have?
• Significant fines from the Information Commissioner and claims submitted for non-compliance with data protection legislation.

What opportunities does this create?
• Increased understanding of the Council's information assets. • Increased transparency and trust with data subjects.

What controls do we already have in place?
• Statutory Data Protection Officer appointed who has implemented a robust suite of data protection policies and procedures. This includes the implementation of a Data Privacy Impact Assessment process and the roll out of mandatory GDPR training. • Updated Retention Schedule in place for the Council and revised Privacy Notices developed and uploaded to the Council's website. • Process in place to ensure that all documents and equipment is identified as part of the office moves process to reduce the risk of a data breach. • Information Governance Group in place to share best practice and ensure continued compliance with data protection legislation. • Participation in voluntary ICO audits and associated follow-up processes.

Net Risk Score	12	Impact – 4	Likelihood – 3

What are we doing to further manage the risk?

Continuation of the roll out of the compliance audit programme across the Council by the Information Governance Team.

There are two compliance audits planned to be undertaken in quarter one and these are related to Health and Adult Services. Work is currently underway to plan the audits for the rest of the financial year and once identified the areas will be scheduled across the remainder of the year.

All employee groups to be set up in the HR system including agency staff, contractors, NHS staff, students and partners to gain better control of IT kit issued and improve data management.

This has been considered as part of the iTrent HR and Payroll project however has not been pursued due to the additional licence costs which would be incurred. Some categories of non-employees are captured in the HR system including those on the IR35 tax scheme and also long term agency managers who need to be set up in the HR system in order to manage their teams.

In order to introduce some level of control, ICT have now developed a workflow around the issue of equipment so that managers need to complete and approve a form for temporary user accounts and all of these have an expiry date. The ICT workflow will then contact managers prior to the expiry date in order to establish whether the account should be closed or whether it needs extending. This is an improvement as to what was in place however there is a need to further extend access to the system to the Procurement Team (so that they can check a contract is in place for contractors), HR (so that they can ensure mandatory training is carried out / DBS in place) and potentially the Risk and Resilience Team (to ensure insurance is in place where required).

The focus at present has been on implementing the iTrent HR and Payroll system and, once this is done, a lead needs to be identified to take this next stage forward for better control of non-employees.

Complete the project to transfer currently unstructured shared drives into Microsoft 365 to better facilitate the application of retention periods.

ICT have completed 68 migrations from shared drives to SharePoint sites with 43 drives left to migrate. At the moment ICT are working with the Commissioning Team and Public Health to migrate their very large drives. With every migration ICT provide full support and training to the whole service.

Consider how emails may be better structured to facilitate the application of retention periods.

The UK GDPR requires the Authority to retain personal data 'for no longer than is necessary' which in practice means the Authority must adhere to a retention schedule. The retention schedule applies to categories of personal data as opposed to the format in which data is held. Although the application of retention in email accounts is addressed in the Information and ICT Security Acceptable Use Policy and Records Management Policy, it remains an area of concern for the Council's Data Protection Officer (DPO).

The Council's DPO and Head of ICT Services agreed a phased plan to address the retention of electronic

data that commenced in 2021 and email retention is in the final phase which the DPO anticipates will start by the end of this financial year.

Target Risk Score	8	Impact – 4	Likelihood – 2

What will these additional actions achieve?
Good data protection arrangements ensure that the Council continues to comply with the regulatory framework, therefore reducing the risk of reputational damage, significant monetary fines and importantly protecting the rights of our data subjects. The implementation of the actions identified in the strategic risk register will help further strengthen the Council's approach to the effective protection of personal data.

What barriers do we face?
The Corporate Leadership Team support the work of the Information Governance Team which helps create a culture of taking data protection seriously. However, the barrier to implementing the identified actions is the availability of resources.

Do these actions contribute to the sustainability of the Council?
The Information Commissioner can issue a monetary penalty for failing to comply with the Data Protection Act which could impact on the financial sustainability of the Council if a significant breach occurred.

Do these actions impact on the Council's finances?
The Information Commissioner can issue significant fines for a data protection breach. As the Council strives to adhere to the legislation, fines would be unbudgeted and would impact on the Council's financial position. Furthermore data subjects are able to make a civil claim against the Council should they feel that they have been harmed by a data breach. If a claim was successful the service whose activity resulted in the breach would be required to fund the first £50k – a system which has been introduced as a deterrent for poor practice in service areas. Any costs exceeding this limit would need to be funded from the Council's reserves.

How does this contribute to the Council Plan?
The robust management of personal data is an important part of organisational resilience.

Any links to other strategic risks?
Information and Legal

Any additional changes to this strategic risk?
The Data Protection and Digital Information (DPDI) Bill was re-introduced to Parliament in its second form in March 2023. The DPDI Bill was first introduced in the Summer of 2022 and paused in September 2022 so *'ministers could engage in a co-design process with business leaders and data experts – ensuring that the new*

regime built on the UK's high standards for data protection and privacy, and seeks to ensure data adequacy while moving away from the 'one-size-fits-all' approach of European Union's GDPR.'

Risk: c) Inability to undertake business critical activity due to software failures.

Risk Owner: Director of Resources

Gross Risk Score	20	Impact – 5	Likelihood – 4

What impact does this have?

- Inability to undertake business critical activity due to software failures.

What opportunities does this create?

- Fit for purpose software in place which meets business needs.

What controls do we already have in place?

- List of critical systems and system administrators in place.
- Disaster recovery plans in place for IT systems.
- Staff training of business critical systems to ensure compliance with key controls.
- IT representation at the Corporate Risk Management Group to discuss potential system risks.
- Knowledgeable IT team in place to support services with key system issues.
- Office spaces adapted to facilitate hybrid working through the use of technology.

Net Risk Score	15	Impact – 5	Likelihood – 3

What are we doing to further manage the risk?

Assess the budget that is available to look for provisions for data centre refresh in the coming years to continue to provide resilience and sustain arrangements.

An infrastructure budget is in place and there is adequate funding in the short term and this will continue to be reviewed as part of the budget setting process. It is difficult to forecast future need due to the shifts and changes in technology and, in the future, action will need to be taken to look at ways in which the data centres could be more sustainable as part of the net zero agenda which is likely to require more investment over and above what is held in the reserve.

Implement phase two of the HR and Payroll project.

Phase one of the project went live in November 2022 which included core HR, Payroll and Learning and Development. This phase of the project is still embedding and issues identified on implementation continue to be resolved.

In terms of phase two, the process of paying for eye sight tests has now gone live and work is ongoing to develop the accident reporting system which will hopefully go live in the coming months.

There are some elements which have not been included in the project and a corporate decision will be

taken on whether this will be included in phase two or whether existing arrangements are robust enough and these include:

- Recruitment;
- Managing the establishment for budget purposes;
- Performance management; and
- Time recording.

In some instances existing arrangements are considered more robust then what iTrent offers and therefore consideration will be given to the pros and cons of moving these to iTrent over the coming months.

Implement phase two of the finance system project including Adult Social Care billing.

Phase one of the new finance system went live in April 2023 with key modules such as creditors, debtors, general ledger and banking being launched.

Planning is now underway for phase two of the project which will include the implementation of modules including budgeting, inventory, assets and interfaces (of which Adult Social Care billing is part of). Work on phase two implementation will take place during the next 12 – 18 months.

Develop the Mosaic social care system to enable payment of invoices in a transparent way with adequate control.

A task and finish group has been set up by Children's Services with representation from Finance and IT in order to address the weaknesses regarding the payment of invoices.

At the last meeting the layout for the online forms which will be in Mosaic were finalised. The online forms are going to be how an order is requested and gets the correct approval before the service/purchase is made. Steps are now being taken to resolve some issues around the coding/categories, and how this will work with the new finance system.

Work is underway to update the Scheme of Delegation so this can also be linked into the authorisation in the new finance system.

Phase out the use of analogue phones and move to the use of digital phone lines.

Several projects are underway to address this, these include:

- A project by Property Services to find an appropriate solution for building alarm systems which are currently analogue. Options are being considered with one being the use of SIM cards.
- A project in Vitaline for the telecare system which is dependent on analogue lines. This has been somewhat delayed as the software provider has yet to provide a digital solution.
- A project in Blackpool Coastal Housing to move the warden system from analogue to digital.
- A project by ICT to identify all Council BT lines and decommission these where appropriate or transfer them onto the main digital telephony system where the lines are still required.

Target Risk Score	10	Impact – 5	Likelihood – 2

What will these additional actions achieve?
Having robust software solutions for our key systems helps improve resilience, particularly as these systems will be hosted in the cloud. In addition, the new systems should improve efficiency by enabling better access for self-service for employees and managers and also providing the opportunity to review existing procedures to ensure that these are robust. For the majority of Council systems the impact of loss would not have a risk score of 5 however as some systems are critical, such as Vitaline which is a 24/7 emergency service, the loss of systems could be catastrophic.

What barriers do we face?
As with all new systems there have been some issues arising with implementation which need to be resolved and this will impact on phase two progression is some cases.

Do these actions contribute to the sustainability of the Council?
Having access to robust and resilient core systems helps ensure that sustainability of core services.

Do these actions impact on the Council's finances?
The purchase of software and subsequent software development is expensive and has an impact on staff time. Agreed budgets are in place for the key systems and regular monitoring of these is in place.

How does this contribute to the Council Plan?
Organisational Resilience.

Any links to other strategic risks?
Reputational

Any additional changes to this strategic risk?
The culture change needed in order to embed the new systems particularly in terms of greater self-service by employees and managers.