E10 - Information Security - If there is insufficient security or recovery plans for data held and IT systems used by the councils and resulting in a risk of: a data breach, a loss of service, malicious attacks or inability to deliver services due to loss of systems and data

Inherent risk level		**Lead Member - Councillor Mike Hallam**		**Residual risk level**	
Likelihood	**4**	**Risk Owner - Sarah Reed**		**Likelihood**	**3**
Impact	**5**	**Risk Manager - Chris Wales**		**Impact**	**5**
Inherent risk score	**20**			**Residual risk score**	**15**
		Put the date DD/MM/YY when reviewed in box below↓		**Direction of travel**	
		20/05/21		Identify updated text with red font. Say what columns were updated in box>>>	No change

	Potential impact if risk not mitigated	**Controls**	**Control assessment**	**Mitigating actions (to address control issues)**	**Comments**	**Ongoing COVID impacts**
A1	Loss of critical systems and Service failure	Disaster Recovery Plan in place	Reasonable	New Architecture and Security leads recruited Refresh ICT Strategy following Unitarisation - Review plans and principles for future decisions and to identify any risks	Additional recruitment of information security teams to strengthen the function. A future road map for change and improvement has commenced and shared with ELT	
A2		File and Data encryption on computer devices	Good	We have cyber-essentials plus certification.	Cyber security incidents are inevitable. To manage this risk we have effective controls and mitigations in place including audit and review.	With remote working becoming the norm with the start of the covid crisis, IT have increased efforts to ensure that the Council's data is secure. Multi-factor authentication is now being rolled out and has already been implemented for the
A3		Key business critical systems moved to the Cloud to reduce risk of loss and increase resilience	Reasonable	Eclipse Social Care system moved to the Cloud Cygnum Social care rostering to be moved to the cloud Q2 2021 Other applications to be reviewed for reliability and risk	High priority agreed projects have been mapped by transformation team , working with ICT (as a key enabler) and full assessment of other projects under way to support future development in line with roadmap.	
B	Data loss/ inability to switch to alternative data centre results in significant delays in re-provisioning services	Regular DR tests and Back up of data Development of DR capability within WNC infrastructure of offsite external hosting	Reasonable	Replication and back ups of key data for critical systems ICT WNC DR assessment to be undertaken and WNC ICT plan development setting out risk areas and prioritisation of any changes to infrastructure or DR plans		
C	Financial loss / fine due to financial data loss or fraud	Managing access permissions and privileged users through AD and individual applications	Good	Audit programme of checks periodically Reconciliation checks		
D	Prosecution – penalties imposed	Consistent approach to information and data management and security across the councils	Good	Data breach processes and protocols in place		
E	Individuals could be placed at risk of harm	Effective information management and security training and awareness programme for staff. GDPR training on line	Good	Staff training via llearm to be rolled out for WNC staff in 2021 as a refresher	Work being done to look at capability across organsation with regard to Office 365, Teams etc and relevant traning and support provided	
F	Reduced capability to deliver customer facing services	Password security controls in place	Good	Implemented the intrusion prevention and detection system. Multi-factor authentication rolled out in Sep20 for all users, to add additional security to Council system and data access. Members also onboarded.		
G	Unlawful disclosure of sensitive information	Robust information and data related incident management procedures in place	Good	IM and ICT governance board to be set up		
H	Inability to share services or work with partners	Appropriate robust contractual arrangements in place with all third parties that supply systems or data processing services	Good	As above, cyber security training is being rolled out as will GDPR update training for all staff		
I1	Unsafe IT systems which are easy to hack and penetrate / risk to wnc data / fines from ICO/ Reputational damage	Anti Virus checks up to date and all patches applied in timely way	Good			
I2		Appropriate plans in place to ensure ongoing PSN compliance	Good	Cyber Security issues regularly highlighted to all staff in Staff Specialist training for IT staff		
I3		Adequate preventative measures in place to mitigate insider threat, including physical and system security	Good			
J	Data breaches result from the shared use of systems by West and North staff in services where standalone systems not in place	DPIAs in place for all services where systems and data shared between west and north northants and agreed with ICO.	Reasonable	Clear protocols, checks and audit trails in place for systems where shared teams and access		

Loss of critical systems and Service failure

2. Data loss/ inability to switch to alternative data centre results in significant delays in re-provisioning services
3. Missed risk leading to significant harm to customers or staff
4. Unsafe IT systems which are easy to hack and penetrate / risk to NCC data / fines from ICO
5. Unstable back up solutions

Controls	**Adequacy**	**Critical Success**
01. Disaster Recovery Plan Creation and test of a DR Plan	Reasonable	In place and tested
02. Transformation Strategy incorporating IT and digital strategy/ roadmap development	Good	Aligning development work to Council priorities
03. County-wide CIO network	Good	NCC attendance and representation of NCC views and priorities
04. PSN compliance/ policies and procedures relating to firewalls, emails, password protection and monitoring of the	Good	ability to identify threats quickly and take mitigating actions
05. IT project management and prioritization effective oversight of project development, implementation and resource allocation	Good	Visibility of priorities and IT work programme across the organization
Ability to mobilise the workforce to work in more agile ways Use if innovative IT solutions to enable the workforce to	Good	% of workforce operating remotely and collaboratively