Ref	Function	Sub Function	Risk	Likelihood	Impact	Pre Mitigation Risk Score	Mitigation	Control test	Outcome and Recommendation	Likelihood	Impact	Post Mitigation Risk Score
1C	**Data Security**	Data Extracts	Unauthorised data extracts are being run to extract data for non business use or sale to external third parties	2	3	8	Control reports produced from systems to identify data extracts being created and these should be flagged to our data controller to validate that there is a legitimate business reason for these extracts	Test to see if large data file being extracted mailed/uploaded/saved to pen drive raises any flags within the system	Test evidenced that this is not locked down and data files can be e-mail out with no blocking/inspection or alerting- only restriction is file size. No evidence that audit logs from any systems are reviewed to check for data extracts	2	3	8
2C		Portable data storage	Data is downloaded to portable storage devices, pen drives/data sticks etc. without being encrypted and if lost there is a reputational risk	2	2	5	Data extracted to portable devices or being e-mailed should be encrypted	Download sample data file to a pen drive and read the file from a non council PC. Test evidenced that this is locked down- data can only be downloaded if Bitlocker encryption is installed on the pen drive, meaning that the data can only be view from the device if the encryption password is entered	Portable Storage (USB) is locked down by default. Capita provided, Encrypted devices that can be used. Removable media policy should be adapted by the council and issue to all staff and posted in an accessible area	1	2	2/3
3C		Internet access allows the posting of data files offsite	Data files can be posted to cloud storage site such as One Drive etc	3	2	7						
4C		E-mail monitoring	lack of e-mail monitoring could result in restricted data such as customer lists, credit card details etc. being sent out of the business	2	2	5						
5C		Data Storage- sensitive data encrypted	if access to our systems is compromised and sensitive data can be easily read and used if compromised.	3	2	7						
6C		Data back up-Essential services data is not backed up	Q58 Cyber security stocktake- essential service data is not backed up	2	3	8						
7C		Electoral roll security. Security of electoral roll data being share with third parties (e.g. printers, etc.)	Data is compromised and released into public domain. Reputational damage	2	2	5						
8C	**Internet access**	Access is not restricted to work related sites and unrestricted access is allowed to site which may contain malicious software/Trojans/spyware	By accessing these sites users may inadvertently download a virus/spyware onto the council network.	3	2	7						
9C	**IT- Acceptable use policy**	ensure the councils have an acceptable use policy and a process to ensure new starters are obliged to read it and records retained of who has read the policy	employees may compromise our IT security unless we set out clearly the behaviour we expect of them and ensure they have read and understood it	3	2	7						
10C	**Payment Gateway security**	Payment gateway security	Non compliant payment gateway may put us in breech of PCI (Payment Card Industry) rules and compromise our customers card details	2	2	5						
11C	**E mail**	E-mail activity	use of council e-mail to send non council or non work related activity (e.g. personal mail, spam, inappropriate content etc) could result in reputational risk and or possible compensation claims	3	1	4						

Ref	Function	Sub Function	Risk	Likelihood	Impact	Pre Mitigation Risk Score	Mitigation	Control test	Outcome and Recommendation	Likelihood	Impact	Post Mitigation Risk Score
12C	**Activity monitoring/ reporting**	network activity monitoring	lack of sight of the activity on our network could mean we have no sight of the risk activity happening on our network resulting in our network being hacked. Eg could be used to send spam mail, attempts to compromise website, telephone systems could be compromised and abused,	2	2	5						
13C	**Public presence**	Council impersonation websites	customer impact, negative public impact	1	1	1						
14C	**JML process**	lack of a robust JML process could compromise system security and allow ex employees to retain access to web hosted systems after they leave council employment.	unauthorised access would compromise data security	3	3	9						
15C	**Access controls**	Control of access to our systems should be by means of an effective Active Directory which controls users and their access to our various systems NB ensure all standalone systems are included in this	if the Active Directory is not kept updated and linked to our JML (joiners/movers/leavers) process in order to ensure users are removed or access rights are configured correctly then there is a danger that systems can be accessed by unauthorised individuals outside their allocated permissions.	3	3	9						
16C	**DDOS (Denial of services) attacks on our website**		attempts made to compromise our public facing website preventing public from accessing to obtain service	3	2	7						
17C	**Planing files acceptance- risk that we could import virus/spyware/trojan**		Terrraquest- planning portal provider- virus, malware or ransomeware files passed into council via our 3rd party planning site. Are attachments screened before releasing to the council. 2) Terraquest payment systems is not PCI compliant resulting in our customer payment details being compromised	2	1	2/3						
18C	**Visitor WIFI**		if visitor WIFI is not ringfenced and separate from the council network there is a risk it could be used to compromise security of the council network.	2	2	5						
19C	**Mobile devices**		Council Mobile devices not secure- risk of data loss or corruption of device by virus	2	2	5						
20C	**Computer sharing site**		Risk of third party remotely accessing council PCs by using remote access software-we should block sites such as LetMeIn, Teamviewer. Etc.	2	3	8						
21C	**Computer disposal**		End of life IT kit (computers, servers, mobiles, laptops and pads are not cleaned of data pre disposal	3	2	7						
22C	**Webpage vulnerability scanning**		website has vulnerability in it design or configuration which allows hackers to compromise the councils website	3	3	9						

Ref	Function	Sub Function	Risk	Likelihood	Impact	Pre Mitigation Risk Score	Mitigation	Control test	Outcome and Recommendation	Likelihood	Impact	Post Mitigation Risk Score
23C	**Password policies**		if passwords do not comply to a robust secure format and we do not enforce password change on a regular basis there is a risk that password could be compromised. Also check we block concurrent logins from the same user id. (Applies to all systems)	2	2	5						
24C	**Social Media**		Adverse postings or comments by employees on social media may compromise the council and lead to reputational damage	2	1	2/3						
25C	**Remote access security**		Risk of unauthorised access and lack of management information if we do not have secured access controls to support our strategy of an IT environment that not only supports deep collaboration but continues to enable our staff to work flexibly but securely, anytime, anywhere and with colleagues from other organisations.	3	3	9						
26C	**Governance and Controls**		IT security is not defined or delivered to the agreed standards which protect the council and ensure delivery of a service that enables the council to achieve its business goals. Poor governance may introduce risk in our IT services as we may not track and report on contractual obligations in place to reduce our cyber security risk	3	3	9						
27C	**Cyber Incident response plan**		Lack of a Cyber security incident response plan, tested and supported by awareness of responsibilities and actions required in the event of an incident, would leave the council exposed in the event of a cyber security attack.	2	3	8						