Agenda Item 9

Appendix A

Extract from Publica ICT Services Risk Register

Risk Title	**Information Security & Cyber Security**
Gross Risk	**12**
Risk Identified	Failure to control and secure ICT systems and data against unauthorised access including Cyber-crime attack Risk Owner: ICT Audit & Compliance Manager Date Reviewed : June 2019
Potential Consequence	**The Risk consequences includes** • Loss of essential Council & Publica Services • Corrupt data resulting in data loss. • Corrupt machines resulting in system down time. • Loss of internet access resulting in reputational damage • Financial consequences if we were held to ransom.
Net Risk	**3**
Controls in place	**Mitigation in place includes:** • Anti-virus software. • Anti-malware software. • Anti-spam software on email system. • Firewalls. • Security controls in place and continuously reviewed. • Recruitment of new Cyber specialist • Secure copies of data kept off-site to allow restoration of systems. • Staff awareness of ICT security via e-learning. • Password configuration reviews on major applications • PSN compliance assessments • Internal & External Penetration checks • ICT Security Policy Framework reviews
Target Risk	4
Proposed Actions	Proposed further actions and controls includes: Resilient systems to be implemented to allow delivery of ICT systems if main sits locations are compromised. Review to be undertaken of the NCSC 10 Steps to Cyber Security, to include: • Risk Management Regime; • Network Security; • User education and awareness; • Malware prevention; • Removable media controls; • Secure configuration; • Managing user privileges; • Incident management; • Monitoring; • Home and mobile working • Password Policy reviews Patching (updating software to ensure they have no vulnerabilities). Implement Cyber Essentials program.