Assurance Map

Cluster - Digital & Technology

Corporate Risk Register Risk:

1. **Cyber Security: Organisational Environment** - Risk that Aberdeen City Council could, become the victim of a cyberattack through poorly designed or implemented, or an absence of internal, organisational cybersecurity controls (processes, training, etc.).
2. **Cyber Security: Supply Chain** - Risk that Aberdeen City Council's reliance on suppliers to deliver digital products, systems, and services across the organis ation could lead to cybersecurity vulnerabilities.
3. **Cyber Security: External Threat**s - Risk of attack from malicious third-party actors.

Cluster Risk Register Risks:

1. **Climate Change - Digital Infrastructure** - Digital infrastructure will be impacted by adverse incidents caused by climate change (flooding, extreme weather) resulting in disruption to the delivery of council services.

First Line of Defence (Do-ers)	Second Line of Defence (Helpers)	Third Line of Defence (Checkers)

• Trained and qualified staff • IT Security Technologies – devices to filter traffic and protect network, virus control software and domain access rules e.g. Conditional Access and Encryption • Proactive Monitoring & Alerting • Operational procedures and guidance notes • Mandatory Information Governance Staff Training and IT Security Staff Training • Investigation into incidents and breaches • Patch Management • System Change Management process via Change Advisory Board • Threat Hunting • Environmental considerations via DMCB procurement process	• CMT Boards • Council Committees • D&T Senior Management Team (SMT) undertakes review of Cluster Operational Risk Register • Information Governance Group • ICT System Risk Assessments • Data Privacy Impact Assessments • Vendor Management • Policy documentation including, Information and Communication Technology (ICT) Acceptable Use Policy and ICT Access Control Policy, Protective Monitoring Policy • Annual review against Public Sector Cyber Security Framework • Participation in the North of Scotland Cyber Resilience Group • SC3 and NCSC services to monitor infrastructure and emerging risks	• Independent IT Health Checks for PSN Accreditation by Surecloud. Surecloud are National Cyber Security Centre and Check approved. • Independent Penetration testing on internet facing services by Surecloud. Surecloud are National Cyber Security Centre (NCSC) and Check approved. • Public Services Network (PSN) assurance review annually • Registered for NCSC proactive notifications service • Cyber Essentials Plus assurance • Completed Scottish Government Cyber Assurance audit • Internal Audit – Assurance Review of the Cyber Action Plan (06/03/2024)