

**Assurance Map**

**Cluster – D&T Cyber**

**First Line of Defence  
(Do-ers)**

- IT Security Technologies – devices to filter traffic and protect network, virus control software and domain access rules e.g. Conditional Access and Encryption
- Operational procedures and guidance notes
- Mandatory Information Governance Staff Training and IT Security Staff Training
- Investigation into incidents and breaches
- Monitoring & Alerting
- Patch Management
- System Change Management

**Second Line of Defence  
(Helpers)**

- Corporate Management Team (CMT) Stewardship undertakes monthly review of Corporate Risks
- 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

**Third Line of Defence  
(Checkers)**

- Internal Audit overseen by Audit Risk and Scrutiny Committee
- External IT Health Checks for PSN Accreditation
- External Penetration testing
- IT Audits