Report author: Louise Whitworth

Tel: 07891 276168

Report of Director of Resources and Housing

Report to Corporate Governance and Audit Committee

Date: 30th July 2018

Subject: Information Management and Governance – Update on Public Services Network (PSN) Submission

Are specific electoral Wards affected? If relevant, name(s) of Ward(s):	☐ Yes	☒ No
Are there implications for equality and diversity and cohesion and integration?	☒ Yes	☐ N**o**
Is the decision eligible for Call-In?	☐ Yes	☒ No
Does the report contain confidential or exempt information? If relevant, Access to Information Procedure Rule number: Appendix number:	☐ Yes	☒ No

Summary of main issues

1. The Public Services Network (PSN) was set up as an assured route for information sharing by central government, to facilitate shared services and also serve as the assured route for the Government Connects Secure Extranet (GCSx) mail. It acts as a compliance regime that serves as both a commitment to a basic level of information security for connecting government departments and local authorities and also a level of trust between Leeds City Council and other public services.

2. Due to more stringent compliance controls brought in by the Cabinet Office in 2014 the Council are presently unable to meet the PSN certification requirements. The Cabinet Office contacted the Council through the Chief Executive in January 2017, to ensure that the Council brings itself into compliance as soon as possible. The Council's access to the PSN has not been restricted but this would have been a possible consequence if prompt action was not taken.

1. Recommendations

1.1. Corporate Governance and Audit Committee is asked to consider the contents of this report and be assured of the Council's approach to Information Governance and specifically in this case PSN compliance.

2. Purpose of this report

2.1. To provide Corporate Governance and Audit Committee with an update on the current position on Cyber Assurance and Compliance, specifically compliance to the PSN Assurance standard.

3. Background Information

3.1. An independent IT Health Check (ITHC) is an annual audit required to inform PSN compliance. This identifies a number of vulnerabilities with different levels of severity that need to be addressed. In 2017, when the bar was raised, the Council had over 67,000 vulnerabilities. Since then this has been reduced by the work of the Digital and Information Team across the Council to 595.

3.2. A re-application for PSN Certification was made to the Cabinet Office on the 30th September 2017. In November 2017, a mid-year IT Health Check was instigated in order to ratify the Council's position. The results of the ITHC showed significant improvement. Whilst at that time the Council's re-application for certification was rejected, the Cabinet Office recognised of the considerable effort and large amount of work the team had completed.

3.3. Resources were re-prioritised throughout 2018 on compliance work ensuring appropriately resourced Security and Compliance focus.

3.4. A further re-application for PSN Certification was made to the Cabinet Office at the end of May 2018 using the November 2017, mid-year IT Health Check. The residual 'Security Gaps' were detailed and signed off by Tom Riordan, Chief Executive.

4. Main Issues

4.1. PSN certification is relied upon as an assurance mechanism to support information sharing. This can be used as a substitute for other compliance regimes where many of the requirements are the same as PSN. E.g. It has been necessary for the Council to go through the NHS Digital IG Toolkit process to connect to the Health networks which resulted in approximately a cumulative 10 working days of extra work.

4.2. The PSN Assurance Team (Cabinet Office) mandates that each vulnerability found in the ITHC is extrapolated to the estate as a whole and resolved. Those identified as critical or high must be resolved before the Local Authority can be determined compliant.

4.3. Since the re-application to the Cabinet Office in May 2018, the PSN Assurance Team had raised concerns regarding the timescales for the resolution of one specific issue; namely the removal of Access 2003 databases. Moving off

access is not straight forward and would have an impact on services in terms of disruption and service change. The Council have submitted a migration plan to the Cabinet Office for this “sticky issue” and implemented mitigations to protect the estate from Access 2003. A further update on activities has been requested with the Cabinet Office at the end of July to monitor progress against a Remedial Action Plan. Should those activities meet expectations, LCC may achieve certification.

4.4. With the increased Cyber Threat the controls mandated by PSN are deemed as good practise and also appropriate to meet GDPR and Data Protection requirements. The appropriate Digital and Information Team resources have been prioritised on this work. The impact of this may have effected other projects.

5. Actions to Date

5.1. The PSN Remediation Board, with the Head of Information Management and Governance as Senior Responsible Officer (SRO), reporting to CLT and the Senior Information Risk Officer (SIRO) monthly, has made significant progress. The board meets bi-weekly to work through the compliance requirements and close down remediation tasks realised by the ITHC audit. Monthly meetings with the PSN Authority (PSNA) provide them with regular reports about the progress being made by the council. This relationship is strong and supportive.

5.2. Network Attached Devices – The estate is now being actively monitored for vulnerabilities and patched appropriately. Compliancy is now above 90% for Windows hosts (which comprises the bulk of the estate) and which is an acceptable level for the Regulators. 146 unsupported or un-patchable Windows servers have been removed from the estate.

5.3. Telephony – All Polycom devices have been updated and a process has been established to ensure they are kept up to date in the future.

5.4. Solaris / Siebel - All out of support Solaris servers and all occurrences of out of support Siebel have either been removed from the estate or ungraded appropriately.

5.5. Applications – 32 Cloud suppliers have been identified. They have all been contacted regarding their compliance with the 14 PSN Cloud Security Principles. Where suppliers have been found to be non-compliant, work to remediate has commenced. Cloud Principles have been added into technical specifications for all new contracts and renewals. In development is a ‘Cloud Readiness Assessment’ for external suppliers to ensure that they meet the Principles prior to tender. Mobile Device Management – New security controls on mobile devices. Implementation is mature. Completion expected by the end of September with elected members to follow. An exception group has been formulated for elected members to assist with onsite printing.

5.6. Network Segmentation / Authentication – The procurement of a network access control software is complete, implementation is ongoing with policies being

agreed during the month of July 2018. This work is scheduled for completion by November 2018.

5.7. Access databases - The Council relies heavily on a large number of 2003 Access Databases. This software is unsupported and carries a 'critical' score in the ITHC. There are over 300 live databases which need to be migrated to managed systems to ensure services are able to continue without disruption. A plan is in place with proposed timescales for completion by end of December 2019 which has been accepted by the cabinet office.

5.8. A July update has been requested to monitor progress against the documented Remedial action plan. It is possible LCC will gain certification if this work is completed on schedule.

5.9. Recent Engagement with the PSN Assurance Team

Immediately following the May 2018 submission, the PSN Assurance Team raised concerns regarding the timescales for resolution to the 2003 Access issue. Discussions with the Council's Cyber Assurance Team have taken place. Given the comprehensive mitigations Leeds City Council have put in place to prevent malicious activities arising from the vulnerabilities in Access 2003, the PSN have now accepted the timescales proposed.

5.10. The PSN Assurance have requested that we update them on closure of vulnerabilities due in July. All efforts to complete July remediation activities are in place. Following which they will give the Council an indication of whether acceptable levels of compliance have been met.

6. Consultation and Engagement

6.1 Consultation on the development of strategies, policies, procedures and standards are extensively undertaken across a broad range of stakeholders including information management professionals, representatives from all directorates via the Heads of Digital Change and Information Management Board members.

6.2 A Cyber Training session for members took place in May 2018.

7. Equality and Diversity / Cohesion and Integration

7.1. Equalities, diversity, cohesion and integration are all being considered as part of delivering the Information Management and Governance Strategy. This refers to the way training is being delivered as well as how policies will impact on staff and partners.

7.2. CLT agreed the roll-out of Cyber training including hacking and cracking for all procuring managers to ensure further understanding of the estate and acceptance of risk requiring a competent officer.

7.3. The third version of the mandatory managing information training level 1 has been rolled out to all staff in April 2018 which was updated to include an increased emphasis on Cyber.

8. Council policies and City Priorities

8.1. All information governance related policies are currently being reviewed and a dedicated Policy Review group has been established. As part of this review the group will be consulting with internal stakeholders and external peer checking.

9. Legal Implications, Access to Information and Call In

9.1. Delegated authority sits with the Director of Resources and Housing and Senior Information Risk Owner and has been sub-delegated to the Chief Digital and Information Officer under the heading "Knowledge and information management" in the Director of Resources and Housing Sub-Delegation Scheme.

9.2. There are no restrictions on access to information contained in this report.

10. Risk Management

10.1. Should action against the current PSN Remediation plan not be to the satisfaction of the PSN Authority, the Council will have to withstand a number of risks:

- The Head of the PSN has informed the Department of Works and Pensions of our non-compliance. Continued non-compliance could culminate in the switching off of GCSx mail and access to Revenues and Benefits data.
- The Head of PSN will inform the Information Commissioners Officer, which could culminate in the revisiting of the audit conducted by the ICO in 2013 to ensure compliance against the Data Protection Act.
- The Head of PSN will inform the Deputy National Security advisor to the Prime Minister, who would in turn conduct an assessment based on the national risk profile.
- The Head of PSN could instigate an external audit of all our security systems by the National Cyber Security Centre. The Council could end up under partial commissioner control.
- Ultimately, the Head of PSN could instigate a complete 'switch off' from PSN services

NB. Based on where the Council are with this work the risk of switch off is very low.

10.2. PSN certification is relied upon as an assurance mechanism to support information sharing, where many of the requirements request that the Council present a certificate prior to sharing, or evidence alternative, more time consuming compliance work to be completed. This has had an impact already on sharing with Health as a number of the controls required for the NHS Information Governance Toolkit are evidenced by a PSN certificate.

10.3. Further work is being undertaken in conjunction with the Corporate Risk Manager to embed the recording and reporting of information risk monitoring and management relevant to this project. The Information Asset Register project will generate information required and an automated dashboard will be produced to report risk assessments to the SIRO. This will provide the assurance required by the SIRO from the business and will allow risk mitigations to be prioritised.

11. Conclusions

11.1. The establishment of improved Information Management and Governance in the Council's technical infrastructure and improved practice and procedures outlined in this report (with regards to Cyber) provides a level of assurance to Committee that the range of information risk is being managed both in its scope and through to service delivery. It allows the council to work with partner organisations, third parties and citizens in a clear, transparent, but safe and secure way. It helps to protect the council from enforcement action and mitigate the impact of cyber incidents and other Data Protection breaches.

11.2. The Cabinet Office have acknowledged the significant progress the Council has made and that there are clear plans and commitments in place for that which is outstanding.

12. Recommendation

12.1. Corporate Governance and Audit Committee is asked to consider the contents of this report and be assured that considerable effort is being undertaken to rectify the current situation with regards to the Council's approach to information governance and specifically in the case of PSN compliance where significant progress has been made.