Report author: Louise Whitworth
Tel: 0113 37 83978

Report of the Data Protection Officer

Report to Corporate Governance and Audit Committee

Date: 14th December 2020

Subject: Leeds City Council readiness for PSN submission

Are specific electoral wards affected? If yes, name(s) of ward(s):	☐ Yes ☒ No
Are there implications for equality and diversity and cohesion and integration?	☐ Yes ☒ No
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

To provide Corporate Governance and Audit Committee with an update on Leeds City Council's readiness for Public Services Network (PSN) compliance submission.

Recommendations

Corporate Governance and Audit Committee are asked to

- consider the assurance provided in this report and invite the Data Protection Officer to provide an update report in relation to the Council's PSN application at the next meeting;
- note the outstanding concerns in relation to the Council's position in respect of compliance and invite the Chief Digital Information Officer to provide an update report in relation to operational arrangements to ensure compliance.

1. Purpose of this report

1.1 To provide Corporate Governance and Audit Committee with an update on progress on the Council's PSN submission.

2. Background information

2.1 The PSN is the government's high-performance network, which helps public sector organisations work together, reduce duplication and share resources.

2.2 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.

2.3 On an annual basis, every Local Authority must make a PSN submission to the Cabinet Office, to retain PSN certification. In conjunction with this, an external audit (known as the IT Healthcheck), must be undertaken. Any critical vulnerabilities uncovered by the ITHC must be resolved prior to PSN submission, as part of the PSN certification agreement.

3. Main issues

3.1 The 2020 PSN submission was successfully deferred with Cabinet Office due to COVID-19 pressures. This effectively 'extends' the certification without issuing a new one.

3.2 Whilst a deadline for re-subsmission has not been set, it has been agreed with the Cabinet Office that a plan will be submitted by the 31st December 2020, which documents all the outstanding work to be completed and a firm submission date. The plan will be shared with the Chair of this Committee prior to submission to the Cabinet Office.

3.3 The Cabinet Office are very supportive and have corresponded with us to that effort. This correspondence can be shared, on request.

Actions to date

3.4 In August 2020, the Digital and Information Service (DIS) formed a Cyber Team as part of a pilot, with the remit of working to resolve vulnerabilities on the estate that are understood to be 'Business as Usual' work; work outside funded projects for example, desktop and server patching.

3.5 The Cyber Team has made significant progress, embracing a new way of working for Operational Services. A number of systemic issues have been unravelled, addressing at source, an issue that was preventing 1500 laptops from patching. The focus this team provides is enabling speedier resolution of configuration errors. Vulnerabilities are addressed in a prioritised approach in order to reach compliance across the majority of the estate prior to PSN submission.

3.6 This Cyber Team has been approved to continue until the new Chief Digital and Informastion Officer (CDIO) comes into post (on 23rd December). It is the recommendation of the Data Protection Officer that this Cyber Team and its agile approach to working continues and this recommendation will be put to the CDIO on his commencement of employment.

3.7 There are a number of projects that have slipped due to COVID and resource pressures. Some of these have implications for PSN compliance. Whilst compliance is a priority for the Digital and Information Service, those individuals employed on PSN remediation projects still do so alongside other Council priority projects, Covid projects and business as usual tasks. New priority projects are continually brought to DIS for implementation, therefore, resources are often spread across a number of projects. There is also a risk that the Council's budget pressures and subsequent staffing reductions, will further impact.

3.8 **Projects with an impact on a compliant PSN submission**

These projects have been coloured coded to indicate the level of risk and subquently a negative impact on the Council's submission (Red = high, Amber = Medium, Green = Low)

A brief explanation of each project is given in Appendix A.

Project Name	Rating	Comments
Access Replacement Project		Significant progress has been made. Cabinet Office has agreed future approach
Avaya / Sabio Platform Upgrade		Project was due to complete in December, however due to issues with the supplier the project has slipped to March 2021. This has been raised as a significant risk with the Interim CDIO and with the Director for Resources and Housing (SIRO).
ESP Windows Server / SQL 2008 Upgrade		Extended support gives a compliant position for this years PSN submission. Servers will fall out of extended support next year. The upgrade project will need to be tracked otherwise this will become an issue for the 2021 PSN submission.
Active Directory Raised Privilege Management		Agreed plan in place to complete the work by August 2021. Analysis currently in progress, however no resources assigned to build, which could lead to delays.
Network Access Control Phase 2		Suspended for this period and projected effort moved to keeping the network/security infrastructure working as LCC staff largely moved to homeworking. Also a dependency on BT, who have committed to completing work they need to do by end Dec 2020. In our previous PSN submission, LCC committed to the improvement. Non-completion will be taken into account when assessing our mitigating factors. The Head of Stategy and Solutions is working to address resources.
CMDB/Asset Register Development		Produce design High level design complete - awaiting resource. This will not impact on this year's submission, but will be raised as a 'security gap'.
Information Asset Register Correlation		Produce design – awaiting resource contingent on the above.

3.9 **Governance Structure for Security and Compliance (Cyber) and Information Management**

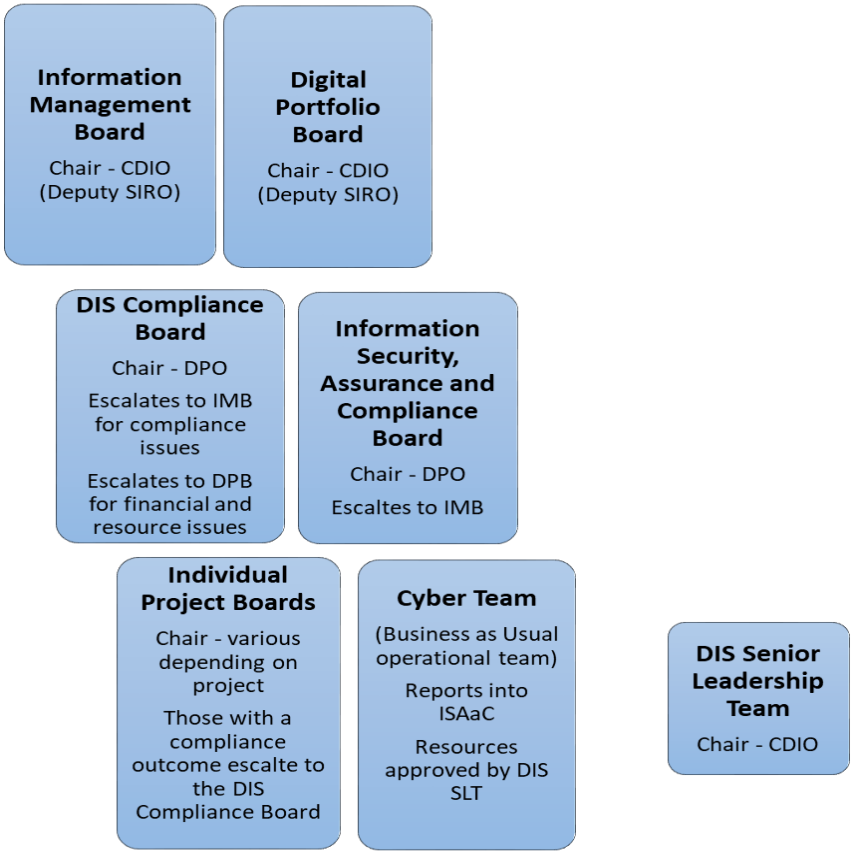
3.9.1 Through the course of the summer, new governance arrangements have been established. A Compliance Board, chaired by the DPO, is now in place where all compliance related projects should report; escalations here are to the Digital Portfolio Board (for resourcing or financial matters) or to the Information Management Board (for information risk escalations).

3.9.2 ISAaC (Information Security, Assurance and Compliance) Board acts as the operational board for BAU activities and includes assessment of management information to aid in the cycle of improvement approach. This board escalates issues to Information Management Board. (IMB) A new ToR has been agreed at IMB for ISAaC which solidifies the activities to ensure BAU activities are managed to their completion and to aid in readiness for the annual IT Health check audit for PSN compliance.

3.9.3 Both the Compliance Board and ISAaC are Chaired by the DPO to ensure compliance priorities are consistent across both project work and business as usual activities.

3.9.4 The Cyber Team take instruction from ISAaC on direction and focussed tasks.

3.9.5 Cyber Team activities are documented and resource allocation for business as usual tasks are approved at DIS Senior Leadership Team.



3.9.6 These new arrangements are in the early stages of maturity. The Cyber Team is working well and has made demonstrable progress.

3.9.7 The Compliance Board have identified some issues which have impeded these arrangements, and have taken action to resolve these:

- In some cases, appropriate project escalations are still slow in reporting to the Compliance Board. This has lead to delays in taking remedial action;
- Not all project managers have been clear whether the project is a compliance project. This has lead to late prioritisation decisions.
- In order to resolves these issues, the Head of Information Management and Governance is working closely the with Portfolio Team and individual Project Managers to ensure that compliance projects are recognised, prioritised and that reporting is timely and consistent.
- The issue has been raised at the Digital Portfolio Board on the 18th November, where the Interim CDIO gave an instruction to ensure that all projects which have a compliance outcome are clearly designated as such to ensure Project Managers are aware of the requirement to report to the Compliance Board.

4. Corporate considerations

4.1. Consultation and engagement

4.1.1 Significant consultation and engagement has taken place with all service areas, information management professionals, representatives from all directorates via representatives of DIS Hubs and Information Management Board members.

4.2. Equality and diversity / cohesion and integration

4.2.1 There are no issues in relation to Equality and Diversity or Cohesion and Integration.

4.3. Council policies and best council plan

4.3.1 The Council has a wide range of compliance programmes for General Data Protection Regulations, Public Services Network Information Assurance, Payment Card Industry Data Security Standards and Data Security and Protection Toolkit.

4.3.2 Non-compliance may affect the achievement of Best Council Plan objectives and the aims of council policies.

4.4. Resources and value for money

4.4.1 All DIS projects undergo a rigourous evaluation and impact assessment process to ensure value for money.

4.5 Legal implications, access to information, and call-in

4.5.1 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.

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

4.6 Risk management

4.6.1 There is a risk that Leeds City Council will not be in a position to make a compliant PSN submission. The Council may be put into remediation measures by the Cabinet Office.

5. Conclusions

5.1 The Cyber Team has made considerable progress at an operational level to complete tasks and workstreams required for PSN compliance.

5.2 However, due to competing priorities and the Covid-19 pandemic some compliance projects have slipped, which puts the Council at risk of non-compliance.

5.3 A new governance structure for Security, Compliance and Information Management has been developed and implemented.

5.4 This new structure requires more work to ensure it is embedded and all reporting and escaltions go through the correct channels.

6. Recommendations

6.1 Corporate Governance and Audit Committee are asked to

- consider the assurance provided in this report and invite the Data Protection Officer to provide an update report in relation to the Council’s PSN application at the next meeting;
- note the outstanding concerns in relation to the Council’s position in respect of compliance and invite the Chief Digital Information Officer to provide an update report in relation to operational and project arrangements to ensure compliance.

7. Background documents[1]

N/A

[1] The background documents listed in this section are available to download from the Council’s website, unless they contain confidential or exempt information. The list of background documents does not include published works.

APPENDIX A – Brief explanation of projects as framed in 3.8 of the report.

Project Name	Description
Access Replacement Project	PSN compliance is contingent on removing unsupported versions of Microsoft Access. In addition, VBA (Visual Basic for Applications) is no longer supported by Microsoft, which may affect the move to Microsoft Office365. This project will work with services to identify where Access is used and remove the reliance on Access by implementing alternative solutions.
Avaya / Sabio Platform Upgrade	The objective of this project is to upgrade the existing Contact Centre Telephone system which consists of Avaya & Avaya Workforce Optimisation platform. This will provide Leeds City Council with a fully supported and expandable platform.
ESP Windows Server / SQL 2008 Upgrade	This project aims to upgrade unsupported servers and data bases to meet compliance requirements. In 2019, extended support was purchased to ensure compliance, this will run out for some of the devices in in January 2021 and others later in the year.
Active Directory Raised Privilege Management	Raised privilege accounts are those that afford greater authority within the estate, allowing the account holder to make changes to the configuration of devices and services within the council's network. Following an internal audit realising a need for improvement, a project has been instigated which will address the findings of the report. DIS recognises there are other actions required to bring the management of raised privilege to an acceptable assurance control and will continue to close-out gaps beyond the scope of the audit report, but ensuring the audit findings are closed first.
Network Access Control Phase 2	The network access control (NAC) product, which prevents unauthorised devices from getting on to the network, has been deployed within the Leeds City Council environment (Phase 1 of the project completed). All known devices are now understood by the system. Phase two of this project requires remediation networks to be created. Therefore, if a device does not meet the council's predetermined compliance criteria, including patching levels, then it is virtually placed in a separate network, which prevents access to corporate assets. The device will then be patched if identified as a corporate device, or quarantined (will only be granted internet access) until such time as the risk has been reduced, following which the device will be released onto the corporate network.
CMDB/Asset Register Development	A configuration Management Database (CMDB) is a holistic inventory of all the device assets, including software licensing, computers, servers, network equipment etc. It records the relationships between the different components to enable smooth delivery of IT services without disruption. The outcome of this project

	is to bring together all the systems where this information is currently stored into one CMDB.
Information Asset Register Correlation	This project is dependent on the completion of the CMDB/Asset Register development project. The Council already has an up to date Information Asset Register. By bringing in the information management elements in the Information Asset register, into the CMDB it will ensure that the criticality of business information will be better understood.