



**Internal Audit Report
2015-2016**

Data Security (Public Services Network)

**Auditor
Julie Ball
August 2016**

Contents

Audit: Data Security (PSN)
Auditor: Julie Ball

If viewing on-screen, please click on the links below or use the scrolling arrows

1	Introduction.....	3
2	Scope	3
3	Findings.....	4
4	Conclusion.....	5
5	Recommendations.....	5
6	Action Plan – Appendix 1	6

1 Introduction

- 1.1 The Code of Connect compliance (CoCo) was introduced in 2008 to Local Authorities. The Public Services Network (PSN) superseded this in 2013 and is a national framework set out by the Government and managed by the Cabinet Office. Chichester District Council has achieved PSN accreditation since this date which provides an assured network over which Government can safely share both communications and services.
- 1.2 Any organisation that has a business needs to communicate directly with individual government departments through the PSN network, need to achieve certification from the Cabinet Office annually. There are currently 15 services within the council that have email accounts to send and receive secure data through the PSN Network, these include; Electoral Services and Revenues & Benefits who also access DWP data.
- 1.3 The Cabinet Office sets out a series of technical standards that the council are required to meet, in order to secure the certification, these include:
- a. A completed signed PSN Code of Connection – this is a compliance statement that documents how council information technology meets baseline requirements set by central government.
 - b. A completed PSN Code of Connection Annex B - evidence of compliance to the conditions above to include, governance, technical interoperability (the capability of different programs to exchange data via a common set of exchange formats), service management and information assurance.
 - c. A completed PSN contact details form.
 - d. IT Health Check (ITHC) document - Testing is carried out for any vulnerabilities on the council's network and the security of East Pallant House by external providers SureCloud. A report was received in December 2014 with a number of recommendations.
 - e. A network diagram (An up to date diagram of the council's network infrastructure).
- 1.4 A PSN connection compliance certificate may be withdrawn at any time the council no longer meets the required standards.

2 Scope

- 2.1 The scope and objectives of the audit were to ensure that:
- the PSN compliance checklist and all supporting documentation is available and up to date, and
 - there are documented processes in place for the responsibility of recording responses and review, prior to PSN submission for certification

3 Findings

- 3.1 The process of PSN accreditation is required to be completed and submitted on an annual basis before the deadline. The council received an email communication from PSN dated 14th January 2015. This stated that, *"We're writing to remind you that your current PSN compliance certificate will expire on 03/02/2015"*. They also write *"As there's now less than 1 month until it expires you should send your PSN compliance submission to us urgently to make sure you get your new certificate before your current one expires"*. The council's submission was sent on 27th January 2015, five working days prior to expiry of the current PSN. Cabinet require the PSN submission to be submitted at least a month before the expiry date to ensure that the council always has a current certificate.
- 3.2 Audit was informed that prior to submission, senior managers were walked through the process and discussed any issues and work in progress at the time. They also considered the impact of additional work on resources in relation to the ICT Work plan together with the associated risk. However, there is no documentary evidence to support these discussions or confirm any actions required.
- 3.3 The Cabinet Office sets out a series of technical standards that the council needs to meet in order to secure the accreditation. Testing found that all the required data sent to the Cabinet Office had a validation check carried out before being allocated to an Information Assurance Assessor for further checking.
- 3.4 The submission for PSN accreditation sent on 27 January 2015 was declined. A further three submissions dated 9th February, 16th March and 15th June 2015 were presented before the PSN team were satisfied that any deficiencies had been mitigated or addressed before issuing a certificate. However, it is worth noting that there was no suspension of the current certificate made during the period. The PSN reported on three occasions that the decline was due to several high/medium findings in the ITHC remediation plan that have not been addressed or were planned to be addressed but that needed to be resolved. It was also due to a number of statements completed by the service that were not accepted by the PSN as mitigation or a reduction in risk.
- 3.5 The council made its fourth submission on 15th June 2015 and received certification on 10th July 2015, some five months after the original submission. This delay was partly due to the time taken by the Cabinet office to review the PSN submission and contact the ICT service with any observations and questions and partly due to changes being made by the service to address recommendations from the Cabinet office. The PSN team worked closely with the service to identify remedial action and agreed an achievable time frame for implementation.

- 3.6 The Commitment Statement was signed by the Chief Executive, Section 151 Officer and the Senior Information Risk Officer (SIRO) stating that the council will work with Cabinet throughout the compliance process and period of the connection to the PSN to ensure the ongoing security of the network. For each submission a signed statement was completed as required. However, for the 2016 submission only Paul Over the SIRO was required to sign the statement.


4. Conclusion

- 4.1 The service has recognised that there were recommendations from the Internal & External Health Check that were outstanding and required addressing to show that the risks have been mitigated. A formal and timely review prior to the original submission may have eliminated the number of rejections received. Therefore the implementation of a PSN review process needs to be put in place.
- 4.2 The application was submitted to Cabinet some 5 days before the expiry date of the council's PSN certificate. This did not allow sufficient time for PSN to carry out a validation check and for an Information Assurance Assessor to carry out detailed checks before issuing a certificate. The service needs to ensure that their next submission is sent at least 20 working days prior to the expiry date of the current certificate. This year the submission was sent on the 10th June and this requirement met.
- 4.3 It is worth noting that no serious observations were reported by the Cabinet Office as this would have resulted in the PSN access being denied to the Council. It is also worth noting that not all vulnerabilities can be addressed at the time of submitting the PSN report due to business dependencies and external factors. However, the Cabinet Office does expect to see that the recommendations from the ITHC have been addressed with suitable mitigations in place to manage the risk presented.


5. Recommendations


- 5.1 An Action Table has been produced, see Appendix 1. In order to prioritise actions required, a traffic light indicator has been used to identify issues raised as follows:
- Red – Significant issues to be addressed
- Amber – Important issues to be addressed
- Green – Minor or no issues to be addressed

6 Action Plan – Appendix 1

Paragraph Ref	Recommendation	Officer	Priority	Agreed?	Comments	Implementation Date
3.3	A formal process should be adopted so that the PSN submission is carefully reviewed on a timely basis before being sent off for certification and evidenced.	ICT Manager	 Significant	Yes	The ICT Manager has confirmed that an Audit Log has been introduced for all communications with PSN. In addition they will be putting in procedures to ensure that the PSN is not only monitored but checked before submission and any recommendations are actioned.	September 2016

Traffic Light Key

Significant Issues to be addressed 

Important Issues to be addressed 

Minor/No issues to be addressed 