The IT Health Check for PSN

An Overview

APRIL 2013

Address Sec-1 Limited, Spring Valley Park, Butler Way, Stanningley, Leeds, LS28 6EA
Telephone 0113 257 8955 ⬢ **Fax** 0113 257 9718 ⬢ **Email** info@sec-1.com ⬢ **Website** www.sec-1.com

Registered Address: Sec-1 Limited, Spring Valley Park, Butler Way, Stanningley, Leeds, LS28 6EA ⬢ **Company no.** 4138637 ⬢ **VAT Reg no.** 764 2446 22

1. IT HEALTH CHECK FOR PSN

Sec-1's standard ITHC testing methodology covers many areas of the PSN IA Conditions by providing your annual External Penetration Test and Internal Vulnerability Assessment, Password Audit and Wireless Network Test. Additional conditions can be covered as necessary.

1.1. BACKGROUND AND OFFERING

What is the PSN?

The Public Services Network (PSN) is the successor to the Government Connect Secure Extranet (GCSx) and Government Secure Intranet (GSi) programmes; aiming to provide a private and secured Wide Area Network to allow electronic communication between public sector bodies at low protective marking levels. The purpose of the PSN remains the same as the GCSx/GSi programmes in that it is a governmental programme to unify the provision of network infrastructure across public sector organisations in the UK aiming to create an interconnected "network of networks" to increase efficiency and reduce public expenditure.

PSN connections are provided to customers – typically local authorities, central government departments and other public sector bodies but this can also include approved third parties within the private sector such as outsourcing providers and any organisation wishing to connect and/or consume PSN services – to enable secure interactions through a common, and standardised connectivity model. In order to become a PSN customer, public sector organisations are required to comply, and annually validate, with the PSN Code of Connection (CoCo).

As the PSN CoCo is an updated version of the GCSx CoCo 4.1 that most public sector organisations will already comply with, transition to the updated standard should be relatively straightforward.

The PSN CoCo is an Information Assurance (IA) mechanism to enable the connection of one accredited network to another, without adversely increasing the risk or affecting the security of the connecting network, or any networks already connected to the PSN. The compliance regime for the PSN CoCo covers a wide range of IT security controls, from patch management to malware protection and system hardening; as-well as non-IT controls such physical security, staff awareness training and protective marking. These IA conditions are present to encourage compliance rather than being a block to gaining PSN access.

The IA Conditions are provided for customers operating between Impact Level 0 and Impact Level 3. The IA controls are identical at each Impact Level, however the application of those controls may vary.

What are the Information Assurance (IA) Conditions?

The IA Conditions provide a risk based approach to information security, and consists of 46 controls into 18 control areas. In comparison to the conditions of the GSCx CoCo, there have been a large number of sections removed and wording clarified to remove specific legacy requirements; focussing on a holistic approach to information security which meets several controls in accordance with ISO/IEC 27001 and also the PCI DSS.

The Customer IA Conditions found in the PSN Code Template Annex B *(available from https://www.gov.uk/public-services-network)* defines the following Control Areas:

- Network Diagrams & Scope (DIA)
- Information Risk Management (RIS)

- Physical Security (PHY)
- Personnel Security (PER)
- User Education (EDU)
- Incident Response (RES)
- Configuration (CON)
- Compliance Checking (CHE)
- Patch Management (PAT)
- Access Control (ACC)
- Boundary Controls/Gateway (BOU)
- Removable Media (MED)
- Malware Protection (MAL)
- Mobile/Home Working (MOB)
- Wireless Networks (WIR)
- Network Obfuscation (OBF)
- Protective Monitoring (PRO)
- Email (EMA)

Condition CHE.1 (Compliance Checking) states the following: "*Organisations shall implement an annual programme of **IT Health Checks** to validate equipment not provided as part of a PSN service that interacts with PSN services.*"

With the retirement of the GCSx standard in November 2012, it is a requirement that any public sector organisations are using the PSN IA Conditions by October 2013. Guidance from the PSN technical transition team advise that a public sector organisations' annual IT Health Check is planned and prepared at least six months in advance of their current CoCo expiring.

What is an IT Health Check (ITHC)?

An IT Health Check (ITHC) is an extremely valuable way of testing whether your systems are being secured against information security risks in accordance with commercial best practice. By ensuring compliance to the CoCo and that IT Health Checks are being performed annually, assurance is given to the overall security of the Public Services Network.

An Information Technology Health Check (ITHC) however covers more than the single penetration test required annually by standards such as the PCI DSS. ITHC's cover all systems connected to, but not provided as part of, the PSN – typically all systems in the internal LAN and WAN within the network of the organisation. ITHC's should also go over and above a simple automated network vulnerability scan, by assessing the overall security posture of the organisation through assessments of protective monitoring controls, user education and remote working devices, as-well as others.

You should expect that an ITHC provides you with an intelligent summary of the findings and recommended actions, rather than simply a formatted dump of the output from automated scanning utilities.

Additionally, an ITHC should be scoped proportionate to the organisation – covering the baseline requirements and additional controls specific to the organisation. For instance, where mobile/remote working technologies are used, an assessment of the techniques to mitigate the risk provided by introducing such devices, such as prevention of data loss through encryption, should be included in the assessment scope. Where appropriate, and ITHC should also cover other IA requirements listed in the PSN Code Template Annex B.

The IA conditions do not need to be in scope for equipment or people that do not access the PSN when separation of that activity is assured. This approach enables organisations to connect to and consume PSN services from an enclave where needed, rather than allowing access from across the entire ICT estate.

Within scope, as a minimum any device, network, person or physical location that connects to or accesses PSN Services that are not already PSN Certified must be considered as targets for compliance.

More guidance on what an IT Health Check means can be found in the PSN FAQ found at: https://www.gov.uk/public-services-network.

For organisations operating at Impact Level 3, a CESG CHECK accredited testing provider is required. The CESG Standard for IT Health Checks is known as CHECK. The CHECK standard was developed to improve the availability and quality of IT testing services provided to Government and public sector organisations. Companies belonging to CHECK are measured against the high standards set by the CESG and are permitted to work on systems processing protectively marked information up to and including CONFIDENTIAL.

CHECK status is conferred to companies by the CESG when they have met strict CESG requirements, and have staff who have attained either CREST (Council of Registered Ethical Security Testers) Team Leader status, or passed the Tiger Scheme certification.

FOR MORE INFORMATION ON THE SEC-1 IT HEALTH CHECK FOR PSN,

CALL 0113 257 8955 | EMAIL INFO@SEC-1.COM | WWW.SEC-1.COM