

Service Definition

PSN Code of Connection (CoCo) IT Health Check

Introduction

G-Cloud customers and Government authorities/departments that connect to the Public Services Network (PSN) must submit a completed Code of Connection annually. A crucial element of this submission is the IT Security Health Check, which is an assessment of the organisation's external and internal networks and how these may impact on the security of the PSN. Typically for Local Authorities, the IT Security Health Check can be conducted by an independent third party that is accredited by CREST.

Intertek NTA is accredited CREST and has extensive experience of providing IT Security Health Checks for local and central Government authorities/departments (also being approved by NCSC as a CHECK 'Green' supplier).

Scoping

A scoping document will be provided prior to purchase of the service to ensure the relevant areas required by Government Digital Services and the Department for Science, Innovation & Technology (GDS/DSIT) are sufficiently considered/included within the service provided. A recommended number of units/days will then be provided to enable requirements to be met.

Service Overview

This service may be purchased either individually or as a collection of services offered by Intertek NTA.

Intertek NTA conduct this service in accordance with IA Condition 7 (Testing Your Security) of the PSN Code of Connection (currently v1.32) and Cabinet Office IT Health Check Supporting Guidance (23rd February 2022), covering the following areas:

- Review topology and PSN network segmentation including network management security (e.g. PSN and boundary/Internet firewalls, access controls, switch configuration)
- Review configuration, build and patching of servers
- Review configuration, build and patching of workstations (desktops, thick and thin clients)
- Review configuration, build and patching of remote access devices (laptops, smart phones, tablets)
- Review configuration, build and patching of remote access solutions
- Review configuration of wireless network(s)
- External penetration testing of Internet-facing services, including remote access solutions

Deliverables

The results presented will be categorised by risk and will provide a clear explanation of each vulnerability, the rating applied (High, Medium and Low), justification of how this rating has been reached and recommendations to enable the vulnerability to be mitigated will be provided.

The report will also consider the sum of all issues and advise on an overall risk rating, given that a series of lower risk vulnerabilities may combine to present a higher threat.

Service Definition

PSN Code of Connection (CoCo) IT Health Check

The report will include hyperlinks, both for navigation within the report and to access external resources such as CVE details at the NVD website, CVSS score referencing where possible, patches at the Microsoft website etc.

The report will contain:

- An executive overview with business implications and confirmation of the ITHC scope
- A summary of risks identified, ordered from high to low severity
- Recommendations for closing holes found
- Technical details of each issue found
- Full listing of test results tables including background information/evidence to support results

A technical telephone debrief is available and included as standard following delivery of the report, to explain the areas covered during the IT Health Check and the key findings and potential business implication (severity) of the issues found. This will include suggested priorities for the customer to take action against.

Service Management

You will be appointed a dedicated account manager and provided with points of contact for commercial and technical questions, to ensure that the service is properly executed.

Intertek NTA has a Service Level Agreement that is monitored by a R.A.G system to ensure that delivery standards are met on all projects. The SLA includes timeframes for project delivery with technical staff working to targets to ensure that deadlines are met.

Additionally, Intertek NTA has a customer services department that is responsible for the key administrative aspects of delivery such as liaising with you to confirm site details, scheduling the test, ensuring reports are sent out in a timely manner, scheduling follow up tests and debriefs etc. This is documented and monitored through the use of an internal database system, and links into other key processes regarding the correct method of sending the report according to the protective marking of the contents.

Information Assurance

Intertek NTA is security cleared to perform IT security testing services on infrastructure, platforms or software containing data protectively marked up to OFFICIAL-SENSITIVE

Ordering and Invoicing Process

Once the scope of work and number of units/days required has been agreed between the customer and Intertek NTA, a valid purchase order is required to enable scheduling and delivery.

An invoice will then be raised upon delivery of the service.

Customer Responsibilities

The customer is responsible for the completion of a Technical Details Form (TDF) prior to delivery. The provision of appropriate information will ensure that delivery meets expectations and requirements.

Service Definition

PSN Code of Connection (CoCo) IT Health Check

Technical Requirements

The resources typically required from the customer to ensure the service is performed as efficiently as possible include:

Internal testing:

- The remote testing environment would consist of a minimum two machines (depending on how many consultants are conducting the test more than one Windows machine may be required); 1 x Linux Kali and 1 x Windows 10/11 (or Windows Server). The Kali machine is where most of the testing tools are installed, the Windows machine will be for RDP access to other Windows systems and possibly some testing tools.
- Intertek NTA's preferred approach is enclosed as a separate attachment. Also included are network diagrams to illustrate two possible options for a remote testing environment. If we are unable to use this preferred approach it may incur additional set-up costs.
- Intertek NTA testing laptops can be sent onsite and connected to the internal network providing VPN access can be provided to them.
- Internal IP address ranges (incl. PSN network, DMZ, corporate, etc.) in scope of testing
- A list of Windows Active Directory Controllers
- A list of critical servers connected/related to the PSN
- A list of other servers to be thoroughly tested and audited
- Firewall details, incl. the configuration and rule base for the firewalls in scope (PSN and Internet firewalls as a minimum)
- Switch configuration documentation
- Current configurations standards, builds and IT security policies
- An appropriate technical contact available for the duration of delivery, to provide the tester(s) with the logical (or physical if onsite) system access that is required to perform the testing as well as for notification of any high risk issues identified during testing
- Access and authentication details to a workstation to test the PSN from this perspective
- Any testing performed onsite will require a power supply, table and chairs for each of the testers at all locations where testing is to be performed
- Intertek NTA consultants must be able to access the infrastructure, systems and applications in scope of testing via their own test laptops/equipment

External testing:

- Technical contact details for any necessary communication during the testing (e.g. high risk issue notifications)
- A list of target Internet IP addresses (to include publicly accessible services such as web servers, FTP servers, IPsec/SSL VPN remote access)
- Details of all Fully Qualified Domain Names (FQDNs) and any other unique entryways into applications, remote access or other systems for the entire in-scope infrastructure
- Internet router details
- Internet firewall details