

SPECIFICATION

CONTRACT FOR THE PROVISION OF ICT HEALTH CHECK SERVICES

PERIOD: 01/01/2025 – 01/01/2026

ICT Health Checks and Cyber Security Consultancy

Requirements

To ensure the best level of expertise and in line with NCSC guidance, testing shall be carried out to the appropriate standard, and organisations must be accredited to, CHECK.

The successful supplier shall be able to demonstrate a thorough understanding of the Government PSN health check and Cyber Essentials requirements through previous examples of carrying out successful security testing in Local Government IT network environments.

The Provider needs to understand the Cyber Essentials and the CAF (COMMON ASSESSMENT FRAMEWORK) and how this could impact the local authority's cyber security and resilience principles and provide further guidance, if necessary, on improvement activities.

Any systems or configurations that are potentially vulnerable to DoS exploits shall be highlighted in the reports without actually being exploited.

The supplier shall be expected to work with Rosendale Borough Council ICT Team to identify any critical systems which may be adversely affected by any of the testing carried out.

In addition to the standard annual testing within the scope of this contract the Council will also require a daily rate which can be used to call off additional testing days as required to provide supplementary tests as required which may include, vulnerability scans, consultancy, configuration review (This list is not exhaustive).

The selected supplier will be required to sign all Rossendale Borough Councils Security and Data Confidentiality Agreements, involved in the delivery of the test and to all data obtained during the assessments.

6.2.2 Scope of Testing required

For each of the items described below the supplier shall confirm that they shall meet the scope of the requirements and testing methodologies used for each of these testing areas and will be compliant with the terms and conditions of the CHECK scheme.

These tests will provide assurance that internal systems have been configured in a secure manner and are being properly maintained at all times. Where there are a large number of devices it is suitable for the Supplier to suggest sample testing as an acceptable approach.

6.2.3 PSN

6.2.3.1 PSN Background / Overview

The PSN (Public Services Network) is a network operated by several suppliers for government that provides a trusted, reliable, cost-effective solution to departments, agencies, local authorities and other bodies that work in the public sector, which need to share information between themselves.

6.2.3.2 PSN Scope Items

- Internet Footprinting
- External Vulnerability Scan
- External Penetration Test
- Core Switch review / Internal Gateway / Firewalls
- Internal Testing - Network Penetration Test
- Wireless Test
- Remote Site Penetration Testing

6.2.3.3 PSN Timescales and frequency

The Supplier shall provide a breakdown of the required number of days (Excluding call off days) to complete the testing as listed above.

In line with PSN requirements the testing must be carried out no earlier than six months before the Code of Connection return (March 2025) is due and this will need to be factored into the schedule planning as described below

The PSN scanning is required in January / February 2025. In order to meet our current PSN compliance date in March 2025, all annual scans must be completed before the end of February 2025.

6.2.7 Additional Requirements

- ADHOC Testing

6.3 Reporting

The reports for penetration testing and onsite ICT Health Checks must conform to the reporting guidelines provided by NCSC. In summary the Council requires the following details shall be met for each report:

1. One report will be required (covering a minimum 10% of PSN).
2. Individual reports will be required for each individual area tested, as not all areas will be included in the PSN / CE submission.
3. The report shall provide details of the individuals involved in the Health Check
4. The report shall be Protectively Marked as appropriate, with handling measures consistent with the Protective Marking.
5. The report shall communicate the background, scope and context of the Health Check
 - the report shall document the aim of the Health Check (as agreed with Rossendale during scoping)
 - the report shall identify the hosts and devices or address ranges agreed with the customer as the scope of the Health Check
 - any other customer-imposed restrictions that affected Health Check testing shall be made clear

6.4 Project Management

Following the successful completion of this Quotation, the successful Tenderer shall hold an initial scoping meeting with Rossendale Borough Council ICT Services to agree the scope and schedule for the delivery of the tendered services.

The Supplier shall then provide:

- A preliminary plan including terms of reference at contract kick-off
- Agree format the findings will be presented

- Exact timings prior to the commencement of any tests
- identification of the potential risk impacts of each assessment and how the risk of a test having an adverse effect on the target systems will be mitigated by the actions of the testing supplier.

The supplier shall set out how the project will be managed to ensure appropriate liaison with the council's own team and trusted service delivery partners.

7 Award Criteria

Criteria	% = 100
Quoted price	70
Flexibility all testing carried out on Rossendale site and any other additional work carried out for no cost	20
Completion of CE forms	10

All submissions shall be in English and prices in Sterling, exclusive of VAT.