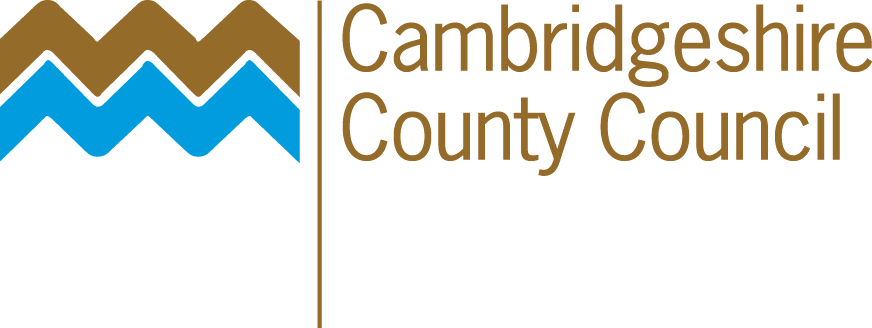
# **REQUEST FOR QUOTATION**

# **FOR**

**Information Technology Health Check for PSN and PCI-DSS.**

**CAMBRIDGESHIRE COUNTY COUNCIL/ NORTHAMPTONSHIRE COUNTY COUNCIL/ NORTHAMPTON BOROUGH COUNCIL/MILTON KEYNES.**

**REF: [XXX]**

3colourcomp

Issue Date: 28th July 2016 NCC/IT, LGSS.

8-10 The Lakes,

Return Date: 12th August 2016 Northampton.

Northamptonshire.

NN4 7YD



The Federation of Small Businesses (FSB) is pleased to endorse this RFQ document. Through changes to their procurement process to support small businesses, Northamptonshire/ Cambridgeshire County Council are showing their commitment to improving the local economy. This positive action is a step forward in the simplification of the procurement process and the FSB look forward to working with Northamptonshire/ Cambridgeshire County Council to encourage effective trade between the Council and local small businesses.

**SECTION 1 - INTRODUCTION**

1. **GENERAL REQUIREMENTS**

Quotations are invited for the provision of Information Technology Health Check, ITHC, for Public Services Network, PSN and, Payment Card Industry – Data Security Standard, PCI-DSS.

The Council’s detailed requirements are defined in Part 2 - Specification.

Please take care in reading this document in particular the Specification; In the event of any questions or queries in relation to this Request for Quotation (RFQ), please contact the named person below.

The Council reserves the right to carry out due diligence checks on the awarded provider.

1. **BACKGROUND**

**Northamptonshire county council IT department, working on behalf of all LGSS members, is looking at procuring a three, 3, year contract for ITHC**.

LGSS is the shared services venture set up by founding partners Cambridgeshire County Council (CCC), Northamptonshire County Council (NCC), and Milton Keynes Council offering a fully integrated support service. The partnership was formed in response to the challenges faced by local authorities, namely, the public sector funding crisis, impact of the recession, rising expectations and growing demand, and seeks to reduce the cost of support services through the consolidation of resources, process redesign and exploitation of technology.

LGSS is governed by a joint committee and began operating legally as a shared service in October 2010. Within LGSS there are four directorates: Finance, Human Resources & Organisational Development, Operations and Legal Services. These directorates provide professional and transactional business services to the two founding councils and a range of other public sector customers.

**Cambridgeshire, Milton Keynes and Northamptonshire County Council work together in partnership under the name of LGSS.**

1. **PROCUREMENT TIMETABLE**

|  |  |
| --- | --- |
| 1. **Request for Quotation Issued** | 28th July 2016 |
| 1. **Deadline for Clarification Questions** | 5th August 2016 |
| 1. **Deadline for Quotation Responses** | 12th August 2016 |
| 1. **Quotation Evaluation** | 19th August 2016 |
| 1. **Contract Awarded** | 29th August 2016 |
| 1. **Deadline for Delivery** | TBC |

1. **CLARIFICATION QUESTIONS**

Any queries about this document, the procurement process, or the proposed contract itself, should be referred to:

Tariq Malik. Supply and Contracts Manager. Email tmalik@northamptonshire.gov.uk

Please note that the deadline for questions is 5th August 2016.

1. **QUOTATION RESPONSES**

Should you wish to take part in the selection process please complete this RFQ and email to:

Tariq Malik. Supply and Contracts Manager. Email [tmalik@northamptonshire.gov.uk](mailto:tmalik@northamptonshire.gov.uk) by 15:00 on 12th August 2016.

1. **EVALUATION OF QUOTATIONS**

Any bids not compliant or completed fully will be discarded. Based on the information provided by organisations, each compliant submission will be evaluated based on the following criteria:

**Evaluation Method: Weighted combination of Quality and Price**

**Quality Questions at 60% + Pricing at 40% = 100%**

1. **Quality Questions (Part 3 Section B)**

Quality Score % will be calculated as follows:

**Total sum of (question score × weighting of question)**

**= Potential Provider Quality Score**

**(Potential Provider Quality Score ÷ Max Quality Score Available) × 40**

**= Potential Provider Quality %**

E.g.:

|  |  |  |  |
| --- | --- | --- | --- |
| **Bid** | **Potential Provider Quality Score** | **Max Quality Score Available** | **Score %**  **(If “*X”* = 40)** |
| Bid 1 | 285 | 300 | 38 |
| Bid 2 | 270 | 300 | 36 |
| Bid 3 | 225 | 300 | 30 |

The Quality Questions will be scored using the following scale:

|  |  |
| --- | --- |
| **Score** | **Criteria to Award Score** |
| 5 | The Potential Provider's response enables the evaluator to have a comprehensive understanding of how the requirement will be met. The evaluator can clearly identify comprehensive evidence that the response given will deliver all stated requirements. The response also demonstrates how relevant **added value** will be provided. |
| 4 | The Potential Provider's response enables the evaluator to have a **comprehensive understanding** of how the requirement will be met. The evaluator can clearly identify **comprehensive evidence** that the response given will deliver **all** stated requirements. |
| 3 | The Potential Provider's response enables the evaluator to have an understanding of how the requirement will be met. The evaluator can identify evidence that the response given will deliver **all** stated requirements.  **OR**  The Potential Provider's response enables the evaluator to have an understanding of how the requirement will be met. The evaluator can identify **sufficient evidence** that the response given will deliver **most** of the stated requirements, but the solution offers added value. |
| 2 | The Potential Provider's response enables the evaluator to have an understanding of how the requirement will be met. The evaluator can identify **sufficient evidence** that the response given will deliver **most** of the stated requirements. The response may have raised one significant concern or one or more smaller issues. |
| 1 | The Potential Provider's response **does not** enable the evaluator to have a clear understanding of how most of the requirement will be met. The evaluator **cannot** clearly identify that the response given will deliver all stated requirements due to insufficient evidence, the Potential Provider’s limited understanding and/ or omissions. |
| 0 | The evaluator believes that Potential Provider has failed to either answer the question or provide a relevant response. |

1. **Pricing (Part 4)**

Pricing % will be calculated as follows:

**(Lowest compliant bid price ÷ Potential Provider's price) × 60**

E.g:

|  |  |  |  |
| --- | --- | --- | --- |
| **Bid** | **Lowest Compliant Bid Price (£)** | **Potential Providers Price (£)** | **Score %**  **(If “*Y* “= 40)** |
| Bid 1 | £45,000 | £45,000 | 40 |
| Bid 2 | £45,000 | £50,000 | 35 |
| Bid 3 | £45,000 | £55,000 | 29 |

Total score:

|  |  |  |  |
| --- | --- | --- | --- |
| **Bid** | **Quality Score (%)** | **Price Score (%)** | **Total (%)** |
| Bid 1 | 58 | 40 | 98 |
| Bid 2 | 55 | 35 | 90 |
| Bid 3 | 50 | 29 | 79 |

**SECTION 2 - SPECIFICATION**

# IT Health Check Specification

1. **Specification for Health Check to Cover PCI-DSS, PSN and Local Requirements**

Note that the specification includes both PCI-DSS and PSN components and that both tests will be in a single health check (other than specific health checks commissioned due to major infrastructure chages.

Where the item refers to CDE this is for the PCI-DSS test but this does not exclude items necessary for PSN or to gain overall security assurance for the organisation.

1. **Who**

PCI-DSS testing will need to be performed by someone qualified to perform PCI-DSS testing.

The ITHC should be performed by persons qualified to CHECK scheme, run by CESG, Tiger Scheme- or CREST-approved.

1. **Reporting**

Both the penetration test methodologies and results must be documented.

**Approach**

A collaborative approach to the test is needed. So any critical issues immediately found are passed to the local IT Operational Manager so that consideration can be made as to whether this vulnerability can be actioned at the time of the test.

To provide an open, collaborative and consultative approach to our requirements: throughout each element of the project, provide daily progress updates, when appropriate, to the agreed contact. These updates will be informal conversations and will summarise the daily activities and progress/completion status of the project together with any security vulnerabilities identified.

Part of these progress updates will be to provide confirmation of the ‘plan of attack’ for the following day’s activities when appropriate. These updates will normally be provided at the conclusion of a day’s activity, unless a high risk vulnerability is discovered in which case the contact will be notified immediately.

If any high risk issues are identified and highlighted during the course of onsite delivery, the consultant(s) will provide a recommendation for remedial action.

If the remedial action is performed whilst the consultant(s) are onsite, endeavour will be made within the remaining time available to confirm the issue has been fixed. In these instances the final report will state that the vulnerability was identified and fixed immediately.

During the testing process, the test engineer must be happy to allow council staff to observe the process, demonstrating where and how key issues may have been found and thus ensuring beneficial transfer of skills as well as establishing a positive and collaborative relationship.

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

The Council will also have access to ‘Vulnerability Help Desk’ for the duration of the contract, to further discuss the issues identified and recommendations made. While this does not extend to the supplier fixing the issues, it does allow a period of time to speak with the vendor about the findings.

Where appropriate feedback on how the findings were determined will be necessary in support of escalation for example to third party suppliers.

**Restrictions**

The tester should explain what actions they are taking to the local IT team.

The tester shouldn’t bring down any service while running their test.

Some LGSS Sites have a policy which states that third party devices shouldn’t be attached to the LAN. If the vendor needs to attach a device to run scripts etc. then the tester should explain why and how any risk can be mitigated or an alternative agreeable method can be agreed ahead of the test.

Where the restrictions are in place a vanilla build laptop can be supplied to the tester in advance for addition of their own tools. This will be in addition to any machine supplied e.g. for build testing or desktop/laptop vulnerability tests.

The tester must undertake not to introduce any malware by attaching a device.

The tester must remove any tools loaded onto a device upon completion of the test.

**Output**

As a minimum the output of the health check should include the following:

* Authors should ensure that the report is readable and accessible to the customer and contain a clear summary of the number, type and severity of the issues identified. Where possible CVSS base scores should be included
* The report should provide details of the individuals involved in the ITHC
* The report should communicate the background, scope and context of the health check in full
* Vulnerabilities should be accurately identified and explained
* A summary spreadsheet of the findings to enable working through the findings and in support of PSN/PCI-DSS submission.

Each identified vulnerability should be associated with a remedial solution. The remedial solution should not be seen as the sole method for reducing the risk - a short-term remedial action may be appropriate until such time that a strategic fix can be put in place.

Typical short-term remediations may include a combination of network segregation, limiting access, increased monitoring and further hardening.

**Retesting Identified Vulnerabilities**

The organisation should take steps to remediate any exploitable vulnerability within a reasonable period of time after the original test. When the organisation has completed these steps, the tester should perform a retest to validate the newly implemented controls mitigate the original risk.

Remediation efforts extending for a long period after the initial test may require a new testing engagement to be performed to ensure accurate results of the most current environment are reported. This determination may be made after a risk analysis of how much change has occurred since the original testing was completed.

In specific conditions, the flagged security issue may represent a fundamental flaw in an environment or application. Whether a complete system retest is necessary will be determined by the risk assessment of those changes

**Identified Vulnerability Reporting**

Penetration test reports should include a discussion of the steps, vectors, and exploited vulnerabilities that lead to penetration during testing for which remediation and retesting are required.

However, it is possible for the tester to identify vulnerabilities that were not necessarily exploitable but which are deemed to pose a potential risk to the environment. It is recommended that the report contain any findings that impact the security posture of the assessed entity even in cases where exploitation did not occur. Some examples:

* Firewall misconfigurations that permit unauthorized traffic between secure and insecure zones
* Detection of credentials obtained through manipulation of a web-application error message that was not flagged during an ASV scan due to a low CVSS base score

**Assigning a Severity Score**

The report should clearly document how the severity/risk ranking is derived.

**Penetration Test Report Outline**

* Executive Summary
  + Brief high-level summary of the penetration test scope and major findings
* Statement of Scope
  + A detailed definition of the scope of the network and systems tested as part of the engagement
  + For PCI-DSS testing clarification of CDE vs. non-CDE systems or segments that are considered during the test
  + For PCI-DSS testing identification of critical systems in or out of the CDE and explanation of why they are included in the test as targets
* Statement of Methodology
  + Details on the methodologies used to complete the testing (port scanning, nmap etc.)..
* Statement of Limitations
  + Document any restrictions imposed on testing such as designated testing hours, bandwidth restrictions, special testing requirements for legacy systems, etc..
* Testing Narrative
  + Provide details as to the testing methodology and how testing progressed. For example, if the environment did not have any active services, explain what testing was performed to verify restricted access.
  + Document any issues encountered during testing (e.g., interference was encountered as a result of active protection systems blocking traffic).
* Segmentation Test Results
  + Summarize the testing performed to validate segmentation controls, if used to reduce the scope of PCI DSS.
* Findings
  + For PCI-DSS testing whether/how the CDE may be exploited using each vulnerability.
  + Risk ranking/severity of each vulnerability
  + Targets affected
  + References (if available) - CVE, CWE, BID, OSBDB, etc. - Vendor and/or researcher
  + Description of finding
* Tools Used
* Cleaning up the Environment Post-Penetration Test

1. **Frequency**

Penetration testing should be performed at least annually and anytime there is a significant infrastructure or application upgrade or modification – this will mean that several health check requests for each organisation may occur in any one year dependent upon infrastructure changes.

1. **Scope**

For PCI-DSS testing the cardholder data environment and all systems and networks connected to it.

**External testing**

This should include systems that provide services on the internet such as email servers, web servers and other systems such as the firewalls that are in place to prevent unauthorised access from the internet into your organisation.

External testing should also include any systems you have in place to allow staff to connect into your organisation remotely. These remote access solutions normally involve VPN that should be tested as part of your external assurance.

Where third-party suppliers have access to and from our systems from their own office locations this should also be considered as an external connection and tested.

|  |  |
| --- | --- |
| **External Penetration Test**  Addresses external aspect of PCI 11.3 and the external test requirement for PSN CoCo  One-off | One-off Remote Assessment  Black Box and Unauthenticated Perspective  (number of IPs supplied) x Active IPs  Manual network and application level check for any vulnerabilities within the target systems  Includes: (list of web sites supplied) and other named web sites hosted at (LGSS sites supplied).  Test performed by CHECK or CESG approved staff |

**Internal testing**

Internal testing should include vulnerability scanning and manual analysis of the internal network. At a minimum it should include:

* Desktop and server build and configuration, and network management security
* Patching at operating system, application and firmware level
* Configuration of remote access solutions (including solutions for managed devices and BYOD)
* Build and Configuration of laptops and other mobile devices such as phones and tablets used for remote access
* Internal security gateway configuration (including PSN gateway)
* Wireless network configuration

The testing should include representative vulnerability scanning across the entire estate covering end-points (including thick and thin clients), servers, network devices and appliances. The scanning needs to include applications on devices; this will be achieved through **credentialed** vulnerability scanning.

A sample testing: where the size of the sample is no less than 10 per cent of the estate can be used – this is for all network attached devices including e.g. switches, printers, desktops, servers, mobile devices.

The firewall will be penetration tested by a CESG Health Check Scheme (CHECK) or CREST.

Full and complete details of the network and applications will be supplied to support testing.

For PCI-DSS testing the scope of an external penetration test is the exposed external perimeter of the CDE and critical systems connected or accessible to public network infrastructures. It should assess any unique access to the scope from the public networks, including services that have access restricted to individual external IP addresses. Testing must include both application-layer and network-layer assessments. External penetration tests also include remote access vectors such as dial-up and VPN connections.

For PCI-DSS testing the scope of the internal penetration test is the internal perimeter of the CDE from the perspective of any out-of-scope LAN segment that has access to a unique type of attack on the CDE perimeter. Critical systems or those systems that may impact the security of the CDE should also be included in the scope. Testing must include both application-layer and network-layer assessments.

For PCI-DSS testing if segmentation controls have been implemented to separate environments, segmentation checks should be performed from any non-CDE environment that is intended to be completely segmented from the CDE perimeter. The intent of this assessment is to validate the effectiveness of the segmentation controls separating the non-CDE environments from the CDE and ensure the controls are operational.

For PCI-DSS testing the penetration test may include systems not directly related to the processing, transmission or storage of cardholder data to ensure these assets, if compromised, could not impact the security of the CDE.

|  |  |
| --- | --- |
| **Internal Code of Connection IT Health Check & Penetration Test**  Addresses condition CHE1 of PSN CoCo and the internal aspect of PCI 11.3  One-off | (number of users supplied) x users (to be supplied by each location on commissioning their health check)  (number of servers and devices supplied) x servers & devices (to be supplied by each location on commissioning their health check)  Sample of devices to focus on those associated with PSN and PCI services and dataflows  Scope to be defined via completion of scoping forms, provision of PSN network diagram and discussion with test engineer  Test performed by CHECK or CESG approved staff |

**Application-Layer and Network-Layer Testing**

Any software written by or specifically for the organisation should be subject to both an application and network-layer penetration test. This assessment helps identify security defects that result from either insecure application design or configuration, or from employing insecure coding practices or security defects that may result from insecure implementation, configuration, usage, or maintenance of software. (Details of any relevant software will be supplied when the individual location commissions their health check).

**Authentication**

For PCI-DSS testing if the application requires user authentication to the custom software, testing should be performed against all roles or types of access assumed by these parties.

**Web Applications**

For PCI-DSS testing a web application that was not specifically coded for the organisation does not need an application-layer penetration test. Instead, the tester should perform a network-layer test and ensure the software was implemented, configured, and is currently being maintained in a secure manner (disabling or uninstalling unused services, blocking unused ports, applying current updates, etc.).

**Segmentation Checks**

For PCI-DSS testing satisfy this requirement by actively attempting to identify routes and paths from networks outside the CDE into the CDE. All segmentation methods need to be specifically tested.

In very large networks, with numerous internal LAN segments, it may be infeasible for the penetration tester to conduct specific tests from every individual LAN segment. In this case, the testing needs to be planned to examine each type of segmentation methodology in use (i.e., firewall, VLAN ACL, etc.) in order to validate the effectiveness of the segmentation controls.

**Additional Tests That Might Be Requested But Do Not Form Part Of The Regular Annual Test.**

**Social Engineering**

Social-engineering tests are an effective method of identifying risks associated with end users’ failure to follow documented policies and procedures e.g. phishing/spearphishing testing on staff.

PCI DSS does not require use of social-engineering techniques,

However LGSS is reviewing its approach towards social engineering tests and may request these in the future.

**Physical Testing**

Currently LGSS does not require physical testing e.g. access to the building/server room/tailgating Or building access system testing however this is being reviewed and LGSS may require this in the future.

1. **Preparation**

**Items We Can Supply To Support The IT Health Check**

PCI-DSS items include:

* A network diagram (1.1.2)
* Results from a QSA review or Self-Assessment Questionnaire (SAQ)
* Annual testing of controls to identify vulnerabilities and stop unauthorized access (11.1)
* Results from quarterly external and internal vulnerability scans (11.2)
* Results from the last penetration test (11.3)
* Annual identification of threats and vulnerabilities resulting in a risk assessment (12.1.2)
* Annual review of security policies (policies that need to be updated may identify new risks in an organisation) (12.1.3)

Documentation from all of the above should be evaluated, and threats and vulnerabilities found as part of the normal assessment processes should be considered for inclusion.

PSN Items:

Details of connections to Third Party Networks

Details of Wide Area Network e.g. CPSN/NPSN

Details of Partner organisations

Details of the main applications in use i.e. the critical ones

Details of satellite offices/libraries/schools connected to the network

**Specification of tests to run**

* Libraries PCs.
* External: assessing the infrastructure that is publicly accessible including Web, Mail, Remote Access gateways.
* Check of online registries to determine information about recorded about (organisation)
* Internet Routing/Router Checks
* DNS Checks
* Firewall Checks
* Internet Server Checks (Identified from DNS Search)
* Checks of hosts identified which are not servers
* Service Checks:
  + SMTP
  + POP3
  + IMAP
  + HTTP
  + HTTPS
  + SSL
  + DNS
  + FTP
  + SSH
  + IKE
  + NTP
  + NetBIOS
  + Citrix
  + Oracle
  + MySQL/Microsoft SQL/PostgreSQL
  + SNMP
  + Sun RPC
* Web application tests (for example):
  + SQL Injection
  + Cross Site Scripting tests – input sanitisation/error handling
  + Directory traversal checks
  + Out of bounds value handling
* Internal: assessing the infrastructure that is accessible from within the (WAN) network including (but not limited to) Web, Mail, Active Directory Domains. The IP address count and VLAN numbers can be supplied on request.
* Organisation foot printing (i.e. the act of determining our network structure from the Internet and from public access points. This should include DNS resolution).
* Port scanning of externally facing servers.
* Discovery of and testing of network management interfaces
* Testing of accessible services advertised by servers
* Unauthenticated user access to detectable file shares
* Patch management checks (using a suitable access account)
* Testing undertaken from minimum number of sites required to test the connectivity between the different VRFs – one school, library and council office (other than head office)
* Application Security Testing Performed from both an external and internal standpoint
  + A relavant application list will be supplied by the location on requesting the test
* All Internet facing firewalls, devices (servers, network devices etc.) and services.
* Wireless networks.
* Websites
* Internal testing of servers and user device standard build images.
* Building Access Systems

The External Penetration Test provides an examination of defined Internet facing IP addresses, testing for configuration, operating system and software vulnerabilities, as well as unauthenticated application level vulnerabilities.

Conduct network probing to identify all systems visible from the Internet within the supplied IP address range(s), including routers, firewalls, web application, remote access systems, mail and domain name servers. Where found, these systems will be tested for vulnerabilities within the operating system, the software and their configuration.

Unauthenticated application level testing would also be conducted against any web-based applications, remote access or file transfer systems found within the specified IP range, to identify flaws such as insecure authentication, weak encryption, SQL injection, faulty lockout facilities and cross-site scripting.

Assess and correlate the findings of the initial automated stage and perform manual verification and further testing of any results that look unusual, any systems that appear to be complex or offering multiple ports, or systems for which there are conflicting results. A key focus of manual testing would be on web applications and remote access systems within the target IP range.

The below tests would be performed if the associated system type is identified:

Manual Check of Web Site – Assess the security of search functions and form submissions on the websites, particularly with regards to data sanitisation controls (before data is submitted back end database) to check for injection and cross site scripting vulnerabilities.

OWA Security Test – Search for vulnerabilities that that may allow an unauthorised user to bypass authentication and access internal mail records, monitor mail traffic or perform a Denial of Service attack against the mail system.

SSL VPN & Citrix Gateway Security Test – This test would seek to ensure that remote access portals are locked down and securely configured, checking that strong authentication and encryption is in place and that the system is not vulnerable.

IPSec VPN Security Test – The objective is to determine as much information as possible about the configuration and security of the target VPN server and to establish if it is possible to gain access to the network through this device. Vulnerabilities are usually caused by poor configuration, particularly with regard to the authentication procedure.

Site-to-Site IPSec VPN – Check that the IPSec VPN system is configured for site-to-site access only and does not allow for remote access from non-specified external IPs and does not leak sensitive system information.

SFTP Test – Determine whether the file upload system is protected from unauthorised use by strong authentication and encryption mechanisms.

The service is engineered to ensure that no damage is caused. Limited exploitation is performed to prove exploits such as cross-site scripting, but with damaging exploits and denial of service attacks not being performed.

Examples of vulnerabilities which might be located include:

* + Unsupported operating system detected
  + Servers allow Windows Terminal Server access
  + Router allows Telnet access
  + Firewall offers dangerous network services
  + Exposed CMS admin interface
  + FTP servers have world-writeable directories
  + SMTP server allows relaying
  + Firewall/Server offers PPTP VPN service
  + Directory Listing available through PROPFIND method
  + VPN system uses crackable transforms
  + Microsoft Outlook Web Access URL Redirection
  + SSL/TLS version (un)supported
  + Remote command execution and shell access
  + Unrestricted file access and download
  + Local administrator password discovered
  + Access to FTP possible with re-used credentials
  + SSL VPN user using weak guessable password
  + Web applications have cross-site scripting vulnerability
  + Web application vulnerable to URL redirection attacks
  + Application backend source code disclosure
  + Authentication credentials found hardcoded in web file
  + Phpinfo.php file leaks information

The IT Health Check will be based on the information provided by the Council, IA Condition CHE.1 (Compliance Checking) of the PSN Code of Connection (v2.7), PSN IA Conditions Supporting Guidance (v1.4), Cabinet Office IT Health Check Supporting Guidance and the external organisations experience of delivering Government IT Health Checks as a CESG CHECK ‘Green’ and CREST accredited company.

The scope of work for the IT Health Check, supported by the Council’s PSN Network Diagram that meets the requirements of IA Condition DIA.1 (Network Diagram), will cover the following activities where appropriate:

The PSN Network Diagram and any associated topology documentation will be reviewed to ensure that appropriate network segmentation is in place and protecting the PSN from unauthorised access.

Additionally, a network summary / enumeration exercise will be performed, with the following objectives:

§ Scan to identify all IP addressable advices on the internal network

§ For each device, report the IP address

§ Basic fingerprinting of operating system

Test across different firewall interfaces to demonstrate firewall restrictions in place between network segments.

Firewall configurations in scope will also be checked for the following issues:

§ The recommended firewall rule set configuration as detailed in the PSN IA Conditions Supporting Guidance (v1.4)

§ Firewall security features disabled

§ Firewall hardening

§ Allow all rules present

§ Blacklisting used rather than white listing

§ Non-specific rules (e.g. lacking source, destination or protocol)

§ Privileged host rules (allowing potential network backdoors)

Perform a review of a servers and a 10% sample of other connected devices (PCs) and tablets/laptops.

Testing is conducted by physically connecting to the test point in the local network.

Testing will include an assessment of patch levels, weak passwords and services offered, as well as configuration, operating system and software vulnerabilities. Test perspectives can include testing from the position of a non-PSN authenticated and/or unauthenticated LAN user, a PSN authenticated and/or unauthenticated user, and from within the PSN segment itself. Testing the defined target from a different network segment allows for the trust relationship between the two segments to be assessed, whereas testing from within the same network segment identifies the system vulnerabilities that an attacker may exploit should they gain direct access to that segment.

Although the assessment will be mostly ‘black box’, the consultant may wish to ensure that those systems that contain the most sensitive/confidential information are subjected to more rigorous testing than less critical areas.

Testing includes, but is not limited to, the following key areas:

§ Patch levels

§ Weak passwords e.g. blank, default or trivial

§ Services offered

§ Configuration vulnerabilities

§ Operating System vulnerabilities

§ Software vulnerabilities

§ Application vulnerabilities

§ Access controls: e.g. unauthenticated access / unrestricted access, access control lists

§ Controls around administrative actions on key systems and how they are managed

§ General user management and network management aspects such as SNMP, and routing protocol usage are also analysed during the testing process

The objective of the tests will be to ensure that the implementation is in line with best practice security principles. This will also ensure that servers are configured in a secure manner and that networks are correctly segregated and protecting the PSN connection from issues such as unauthorised access/privilege escalation.

standard build desktop

Review a standard build desktop from an unauthenticated ‘black box’ perspective and attempt to bypass or crack the boot encryption and protection mechanisms, or the MS Windows authentication. This would include examining the BIOS settings and assessing the password configuration.

Examine each desktop from an authenticated, ‘white-box’ perspective, having gained access with a set of ‘standard user’ authentication details, which would be provided following the black box test. This will include examining the anti-virus and anti-spyware controls and the level of local access to each desktop. Also included will be a review of macros and file type management and file and registry hardening procedures. As a part of this, OS patch management and checking for version and patch updates in applications, such as MS Office will also be covered.

A review of the desktop firewall settings will also be conducted and a local pen-test carried out against the desktop. Internet protection, such as ports allowed outbound to the Internet, proxy-server usage, browser settings and restrictions on Internet content would be examined in line with best practise and the Council’s policy document.

examine the policies that are present on the desktop to see if these can be altered or bypassed in some way, allowing a standard user to escalate privileges to administrator level, and will also include an assessment of patch levels.

A security assessment of a remote access device consuming or connected to PSN services will consist of an examination of the device(s) configured to a typical build to determine to what degree user options have been limited in order to maximise security (e.g. password strength, information leakage).

Where applicable, firewall parameters will be checked to ensure that they are configured as securely as possible, examining how applications such as Internet Explorer behave in conjunction with the firewall and checking for any necessary patches.

Further tests may include some or all of the following (dependent on the device being reviewed):

§ Check whether fingerprinted software version has documented flaws

§ Try to obtain group usernames/passwords

§ Check if, and how, certificates are used

§ Assess what, if any, details may be cached locally on the client

§ Examine the configuration and policy that has been set

§ Check that split tunnelling has been disallowed via VPN client or personal firewall

§ Assess how the server responds to the client e.g. what information may be 'mirrored' back

identify vulnerabilities within remote access servers that would enable a user to sniff traffic, map the drives, change the configuration settings of the system or break out of permissible applications into the PSN.

The review will seek to ensure that the remote access server(s) is secured according to best practice principles and if it is possible to intercept the information going between the client and application. Other aspects considered will include patching, password policy and a review of the network architecture in which the server is located

examine the configuration of a standard build wireless access point (if it allows for connection to PSN services). This will include reviewing the firmware version, any security features provided and the configuration of those features

**Documentation**

For PCI-DSS testing detailed documentation of any components within the scope should be made available to the tester. The organisation will supply the tester with the following documentation:

* A network diagram depicting all network segments in scope for the test
* Cardholder data flow diagram
* A list of all expected services and ports exposed at the CDE perimeter
* Details of how authorized users access the CDE
* A list of all network segments that have been isolated from the CDE to reduce scope (Penetration Guidance PCI-DSS)

1. **Methodology**

For PCI-DSS testing all locations of cardholder data, all key applications that store, process, or transmit cardholder data, all key network connections, and all key access points should be included. The penetration tests should attempt to exploit vulnerabilities and weaknesses throughout the cardholder data environment, attempting to penetrate both at the network level and key applications.

The goal of penetration testing is to determine if unauthorized access to key systems and files can be achieved. If access is achieved, the vulnerability should be corrected and the penetration test re-performed until the test is clean and no longer allows unauthorized access or other malicious activity.

1. **Components**

Include all of these penetration-testing techniques:

Social engineering (currently not required – see above) and the exploitation of exposed vulnerabilities, access controls on key systems and files, web-facing applications, custom applications, and wireless connections.

**Application Layer**

The penetration tester should perform testing from the perspective of the defined roles of the application. The organisation will supply credentials to allow the tester to assume the required roles.

**Network Layer**

Network-layer testing is more suitable for automated testing.

However, simply running an automated tool does not satisfy the penetration testing requirement. Automated tools cannot interpret vulnerabilities, misconfigurations, or even the services exposed to assess the true risk to the environment. The automated tool only serves as a baseline indication of the potential attack surface of the environment. The penetration tester must interpret the results of any automated tools and determine whether additional testing is needed.

For PCI-DSS testing using the documentation provided by the organisation the tester should:

* Verify that only authorized services are exposed at the CDE perimeter.
* Attempt to bypass authentication controls from all network segments where authorized users access the CDE, as well as segments not authorized to access the CDE. (Penetration Guidance PCI-DSS)

**Segmentation**

For PCI-DSS testing the segmentation check should verify that all isolated LANs do not have access into the CDE. The penetration tester should verify that each network segment reported to be isolated from the CDE truly has no access to the CDE. For environments with a large number of network segments considered to be isolated from the CDE, a representative subset can be used for testing to reduce the number of segmentation checks that need to be performed.

# **SECTION 3 - SUPPORTING INFORMATION**

*Note to Potential Providers– You may adjust the size of the following text boxes to suit your response.*

##### SECTION A Organisation and Contact Details

A-1 Name of your

organisation

A-2 Registered office

(if applicable)

A-3 Trading address

(if different from registered

office)

A-4 Organisation

Registration Number

(if applicable)

A-5 Is your organisation a:

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

Sole Trader

Partnership

Public Limited Company

Private Ltd Company

Voluntary & Community Sector

Charity

SME (Small and Medium Enterprise)

Other

If you selected other, please

specify

A-6 What, if any, local

connections do you have with the

County

A-7 If the Company is a

member of a group of companies,

please give the name and

address of the ultimate holding

company

A-8 Name of person to whom

any queries relating to this quote

should be addressed

A-9 Telephone

A-10 Email

A-11 Address

(if different to the Address above)

**SECTION B Questions**

Please see section 6 for details on the weighting and scoring criteria.

| **Question**  **Number** | **Question** | **Weighting (1 = Low, 2 =Med or 3= High)** |
| --- | --- | --- |
| 1 | ***Please provide technical details of the testing that you will***  ***provide – Please ensure that you provide specific answers for points***  ***detailed in the section detailed "Specification for IT Health Check"*** | **Pass/fail** |
| Potential Provider’s Response |  |  |
| 2 | ***Experience + accreditation etc of the team members that will be***  ***undertaking the testing.*** | **3.** |
| Potential Provider’s Response |  |  |
| 3 | ***Internal quality review procedures*** | **2** |
| Potential Provider’s Response |  |  |
| 4 | *Report discussion and distribution.*  o *How and at what stages of the test do you report?*  o *Do you hold closure meetings during engagement period?*  o *Do you alert regarding high priority issues in a timely manner*  *prior to test completion?*  o *Also how will you communicate the report securely?* | **2** |
| Potential Provider’s Response |  |  |
| 5 | *Have you as an organisation suffered any security breaches?* | **Pass/fail** |
| Potential Provider’s Response |  |  |
| 4 | *Do you have repeat clients from other local authorities?* | **1** |
| Potential Provider’s Response |  |  |
| 5 | *What testing methodology do you use?* | **1** |
| Potential Provider’s Response |  |  |
| 6 | *Will you need attach your mobile device/s to our network* | **3** |
| Potential Provider’s Response |  |  |
| 7 | *Assuming 6 – if you need to attach your device to our corporate network please indicate the testing that the device will have been subjected to prior to this. (i.e. what assurances do we have that the device will not bring any additional risks to our network).* | **3** |
| Potential Provider’s Response |  |  |
| 8 | *Please provide full details of the time schedule that you*  *envisage using. Please include a timescale on how long the final*  *report will take to be released.* | **3** |
| Potential Provider’s Response |  |  |
| 9 | *Please provide full details on the format of the final report at*  *the end of the testing.* | **2** |
| Potential Provider’s Response |  |  |
| 10 | *Please provide full details of any support that will be included.*  *Please provide details of who will be providing the support, the*  *supplier or manufacturer. Please provide details as to the split of*  *responsibilities for support between supplier and manufacturer,*  *including responsibility for reporting and escalation of calls.* | **3** |
| Potential Provider’s Response |  |  |
| 11 | *Please provide any further information that will support the*  *proposal and provide any additional information not already*  *covered?* | **1** |
| Potential Provider’s Response |  |  |
| 12 | Having read the specification what community benefits, will your organisation provide as part of your proposal?  Examples include:  1) subcontracting locally.  2) improvements to the county  3) Use of apprenticeships, etc... | 1 |
| Potential Provider’s Response |  |  |
| 13 | The level of insurance required is (insert detail of insurance level here). **£5M**  Can you confirm that your organisation has the required level of cover or is prepared to obtain the level of cover prior to award?  *Officer to discuss with LGSS Insurance team what a sensible insurance level is so as not to discriminate against SMEs..* | **PASS/FAIL** |
| Potential Provider’s Response | **Yes** - have levels of cover already and will continue to for this contract    **No** - but will provide the Authority‘s level of cover requested if awarded contract    **No** - have not got cover and won't provide Authority’s level of cover |  |

# **SECTION 4 – PRICING SHEET**

**Pricing and Costs**

Please insert your costs in the table below. The costs should be broken down into components with a full description of each component and its associated time and costs.

|  |  |  |
| --- | --- | --- |
| [Component] | [Component description] | [Costs (£)] |
| **CCC** | **How many days to conduct ITHC at CCC?** | **?** |
| **NCC** | **How many days to conduct ITHC at NCC?** | **?** |
| **NoCC** | **How many days to conduct ITHC at NoCC?** | **?** |
| **NBC** | **How many days to conduct ITHC at NBC?** | **?** |
| **MKC** | **How many days to conduct ITHC at MKC?** | **?** |
|  | **Total Costs (£):** | **?** |

**SECTION 5 – FREEDOM OF INFORMATION**

Information in relation to this RFQ may be made available on demand in accordance with the requirements of the Freedom of Information Act 2000 (“The Act”) and your organisation details will be disclosed where the expenditure is over <£500 (CCC/NCC)/ £250 (NBC)> as per the Government Transparency agenda. Details of all contracts worth £25,000 or more in total value will also be published on the Council’s website.

Organisations should state if any of the information supplied by them is confidential and commercially sensitive or should not be disclosed in response for the Information under the Act. Organisations should state why they consider the information to be confidential or commercially sensitive.

Please state here any specific information in this RFQ that you do not wish to be disclosed under Freedom of information Act. This will not guarantee that the information will not be disclosed but will be examined in the light of the exemptions provided in the Act.

Insert specific Information here if applicable

**SECTION 6 – SIGNATURE AND DATE**

**Request for Quotation for Information Technology Health Check for PSN and PCI-DSS.**

I the undersigned hereby declare by marking an X in the box:

1. that the information provided is complete and accurate;
2. that the price in Part 4 is our best offer;
   1. that no collusion with other organisations has taken place in order to fix the price;
3. to be subjected to the terms and conditions set out in Conditions of Contract identified in Appendix 1;
4. that no works/goods/supplies/services will be delivered or undertaken until both parties have executed the formal contract documentation as identified in Appendix 1 and an instruction to proceed has been given by the Council in writing.

Name ...............................................................

Position Held ...........................................................

Dated ...............................................................

**APPENDIX 1: CONDITIONS OF CONTRACT**

LGSS Legal Services have drafted standard terms and conditions for the supply of goods and services.

Click on the link below for details:

**CCC and NCC officers**

<http://sharepoint.lgss.local/Pages/Contract-Terms-and-Conditions.aspx>

**NBC officers**

For NBC terms and conditions, please speak to the Procurement team.

Or, when running a mini-competition from an existing Framework you need to make reference to the Terms and Conditions from the original Framework documentation

For complex contracts or contracts of a long duration it is advisable to consult with Legal Services (LGSS Law) for advice on suitable terms and conditions for complex contracts.