RM3764.iii Cyber Security Services 3

Order Schedule 20 (Order Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Order Contract

---

Security Testing Pilot: Invitation to Tender (ITT)

The Local Government Association (LGA)

The goal/ project objective

1. The Local Government Association (LGA) is working with roughly 10% (32) of Local Government Authorities in England to offer a variety of security tests (external, internal and application-based tests) to determine current levels of risk and to produce action plans for improvements.

2. The LGA also wishes to gain an understanding of common issues and levels of vulnerability across the 10%, through uniform reporting of statistical information.

3. The LGA will be using the Cyber Security Services 3 DPS to procure these tests for the 32 participating authorities. These authorities have already been identified and are a representative sample of all English Local Authorities in terms of Type, Geography, and IT profile.

4. This ITT is split into 'lots'. The scope of each 'lot' is described briefly below (4.1 – 4.4), with more thorough detailed information profiles available in Annex A. **We will accept bids for one, two, three or all four of the 'lots' from each supplier. The specification is the same for each 'lot', but responses should be appropriate to the 'lot/s' applying for. The information profiles in Annex A should be useful when assessing costs and scope of each of the tests per council.**

   4.1. Lot 1 – 18 District Councils
   4.2. Lot 2 – 8 Unitary Authorities
   4.3. Lot 3 – 3 London Boroughs
   4.4. Lot 4 – 3 County Councils

Background

5. COVID 19 has resulted in numerous changes within the Local Government sector, as well as on a global basis. In particular:

   5.1. Working patterns have changed to include greater remote working;
   5.2. Together with other workers, technical staff increasingly operate off-site;
   5.3. Solutions have been developed to meet urgent process requirements, often involving personal and special category personal data.

   - These solutions may be based in PAAS environments
   - They may be hosted in IAAS environments, using virtual technology
   - They may be internally hosted.

6. The risk profile has changed in line with these wider changes. This has been acknowledged by The National Cyber Security Centre (NCSC) in their threat reporting.

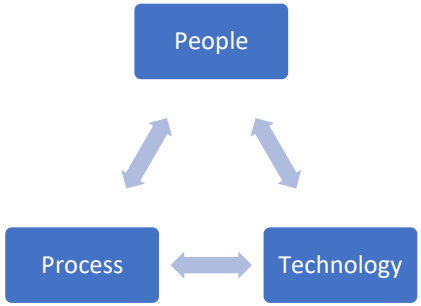
7. Further to this, as the NCSC note, in both their Annual Report 2020 and as published in various media outlets, e.g. the Financial Times and Guardian, the public sector has been a particular target for attack through the pandemic.

The Response

8. Using available funding, the LGA plans to offer selected Local Government authorities the opportunity to conduct security testing as part of a pilot. The scale of the pilot is limited by the funding available.

Benefits to this approach

9. Basics



9.1. Security testing identifies vulnerabilities in information systems which can be exploited by malicious actors.
9.2. Awareness of vulnerabilities provides the opportunity for affected organisations to plan remediation activity, or to highlight difficulties in remediation to leadership and beyond.
9.3. **Technical** vulnerabilities found can highlight issues in business **processes**, and areas where **people** may be more likely to cause damage through their actions (e.g. through activation of ransomware).
9.4. Only a joined-up approach can provide joined-up community information on levels of vulnerability and residual risk, including the ability to lobby for further concentration in this area – and indeed, funding for work – to mitigate community risk.

10. Timeliness

10.1. Wide-scale testing has been a key part of NCSC's response in relation to the NHS[1]. It has been precedented as part of a harmonised approach to current risks. Whilst there is increased access to tooling that may reduce risk, or increase alertness (e.g. WebCHECK, NCSC Early Warnings Service), no similar exercise has been undertaken in this particular space.
10.2. Whilst the majority of organisations undertake some scanning at present – currently due in a large part to PSN compliance – the scope of tests varies, and scans may not be recent (up to 12 months old).
10.3. As such, scans may not cover the current state of Local Government IT solutions. In addition, PSN testing (the "IT Health Check") does not require certain test types – e.g. application tests – to occur.
10.4. The necessity for full IT Health Checks is led by the necessity for PSN compliance in the wider public sector. As the PSN moves towards closure, this requirement will lapse, unless it is replaced by another mandate. Exploration of approaches is beneficial.

[1] https://www.ncsc.gov.uk/annual-review/2020/docs/ncsc_2020-annual-review_s.pdf , p8

The Local Government Body ('Test Subject')

11. Local Government bodies vary in size, nature and technology. However, there are a number of similarities, and it is possible to – in rudimentary fashion – group them into size groups, based on their nature (e.g. district vs county), plus the quantity of technology and devices in use.

12. Internet-Facing services
    All organisations run internet facing services. Whilst traditionally internally hosted and present within a DMZ (there will be external points of presence with services that require testing), an increasing amount of services are run from either virtualised solutions where the organisation has control of the operating system (IAAS) or on platforms such as Azure (AWS and Salesforce are also in place).

    Some solutions are provided by third parties, but usually operate along a similar model (IAAS, PAAS)

13. Traditional End User Devices (PCs, Laptops, Thin Client Terminals)
    Whilst the Local Government environment has traditionally been serviced by PCs, there has been an increasing move over recent years towards thin client, and now to serviced laptops. This trend has been escalated due to COVID.

    Where devices have been migrated to permit remote working due to the pandemic, a number of different mechanisms have come into play for remote access, from traditional full VPN access which might permit traditional penetration testing, through to thin client, through to on-demand VPN for specific solutions. The nature of remote access, plus bandwidth and the need to keep authorities working may impose constraints on the test of End User Devices.

14. Mobile devices
    The use of tablets and phone-based devices is endemic. In the majority of cases, those end user devices are subject to management when corporate, and increasingly when used as BYOD.

Approach – What we want to test for

15. Other test regimes exist, and most of local government already undertakes testing. It is important that our proposed tests build on existing assurance, either by covering areas which may have received less attention, or by providing more timely assurance. The following table identifies existing test regimes, their limitations, and outlines the proposed LGA approach.

SCOPES à	**External vulnerabilities:** *IAAS hosted solutions (e.g. AWS, Azure, Rackspace)*	**External vulnerabilities:** *organisational network + VPN/third party access*	**Internal vulnerabilities:** *credentialled scan*	**Device Builds**	**Remote access config testing**	**Security gateway ('firewall') review & Wi-Fi**	**Web Application testing** *including PAAS*
"Health Check" (PSN)[2]	*Option for penetration test*	*Full penetration test*	*Penetration Test - aims to cover all, but 10% sample minimum for larger orgs.*	*Yes*	*Yes*	*Yes*	*No*
Cyber Essentials+[3]	*Vulnerability Assessment (if deemed in scope by tester)*	*Vulnerability Assessment*	*Vulnerability assessment - "representative of 90% of … devices in scope" – i.e. potentially 1 of each*	*No*	*No*	*No*	*No*
LGA Approach	Full penetration test *Ensures coverage of*	Full penetration test *Updated assurance*	Penetration Test – aims to cover all, but 10% sample	Mobile device risk/compliance checks only.	No *Specialised, out of budget.*	No *Specialised, out of budget.*	Yes – identifiable vulnerabilities + Authentication, Authorisation (AA)

[2] ITHC Supporting Guidance: https://www.gov.uk/government/publications/it-health-check-ithc-supporting-guidance/it-health-check-ithc-supporting-guidance

[3] CE+ Illustrative Test Specification 2.0 https://www.ncsc.gov.uk/files/Cyber-Essentials-Plus-Illustrative-Test-Specification-April-2020.pdf

	cloud migrated infrastructure.		minimum for larger orgs. *Updated assurance, potential to cover hosts not in PSN scope.*				*Achievable scope, basic vulnerabilities + fundamental AA flaws.*

How our approach will complement existing assurances if present

16. Where a PSN IT Health Check has occurred, the proposed LGA approach mirrors it, in terms of external and internal vulnerability analysis.

    16.1. It brings these checks up-to-date, and;
    - It covers a further 10% (minimum) of internal devices, potentially in addition to those scanned previously, uncovering new vulnerabilities.

    16.2. In addition, where organisations have built cloud infrastructure – such as IAAS hosted virtualised servers on AWS or Azure, these are included in the LGA scope.

17. Where organisations have undertaken Cyber Essentials+ assessment, the LGA approach largely covers those areas in greater depth, with manual penetration testing in addition to vulnerability assessment, across a wider range of devices.

18. There is no current mandate for organisations to undertake Web Application Tests, other than that implied by the GDPR/Data Protection Act (DPIA), and as such the test offering here may be new to some organisations. This ties in directly with the concept of new web-based services being launched to cope with the pandemic.

Tests and Scope of Tests

19. COVID-19/Sensitive web application security assessment

    19.1. Organisations have deployed web applications and solutions as part of COVID response, which would benefit from testing. For organisations who have not, there are still web applications processing sensitive information, which would benefit from testing.

    19.2. The scope:

- Assess one to two web applications nominated by the test subject for security testing, with knowledgeable assistance provided by the test-subject. The applications will either have been created for COVID-19 response, or will process significant sensitive data. Applications will be either delivered from test subject's own hosting (internal/IAAS) or PAAS.
- Test scope to determine, for the agreed applications:
    - Common vulnerabilities and flaws, including the OWASP top ten. This may be delivered through automated testing with manual verification, and supplemented by appropriate vulnerability assessment if beneficial & not covered elsewhere.
    - Flaws in authentication, authorisation – a limited time exercise, in conjunction with the test subject, to validate authentication occurs correctly, and roles are enforced.
- If multiple applications are covered, it is not necessary to produce a single report per application, combined reporting is acceptable.
- If the test subject were to wish for additional testing beyond the scope, we would assume an agreed day rate would apply, and that the test subject would seek to fund this themselves.
- Contributes to the overall statistical report (Aim 5)
- **NOTE: this test may be removed from scope or reduced in scope dependent on overall budget constraints. Therefore, the cost of this element should be included separately as an optional cost, with costing per application across the lot.**

20. Internet-Facing service penetration test

20.1. Local Government bodies have varying numbers of external IP addresses within their ranges. The cost of the test should not focus on IP ranges, but be based around the likely number of solutions that will be discovered. We estimate that up to 20% of the server solutions listed in **Annex A** are externally facing.

20.2. We do assume that IP range scanning will occur as part of the initial exercise and anticipate that a sense of scale for this can be derived from the size profile and details provided in **Annex A**.

20.3. Within the scope:

- Conduct vulnerability assessment and subsequent penetration testing on the external network presence of the test subject, bearing in mind the test subject's size and scale.
- The testing should include IAAS instances, subject to approval from impacted parties, which will be arranged by the test subject in conjunction with yourselves.
- Whilst not a formal 'CHECK' test, the penetration test should be conducted to the level of thoroughness required by CHECK standards.

- Contributes to the overall statistical report (Aim 5).

21. Internal penetration test

21.1. It is vital that vulnerabilities be discovered on the non-public elements of the test subject's infrastructure – this includes internal/DMZ hosted services, and solutions only available from the 'internal' side of the network (which may be IAAS/PAAS). The test should also include End User Devices – subject to restrictions imposed by working patterns for COVID-19.

21.2. The scope:

- Conduct vulnerability assessment and subsequent penetration testing on the internal/DMZ networks of the test subject, bearing in mind the test subject's size and scale as shown later. We have assumed that IP scanning is included, and can be factored into overall costs based on the size profile of the test subject.
- The testing should include all server instances, including IAAS and PAAS solutions only available internally, with the co-operation of the test subject.
- The testing should, in co-operation with the organisation, identify whether there is the potential for compromise of 'last resort' backups, in the context of ransomware attack.
- The testing should include traditional EUDs (PC, Laptop, Thin-Client device).
- The test provider may choose, in conjunction with the test subject, to sample areas of the network and/or device types, including EUDs to achieve best value. The sample should be representative in number and device type.
- The test provider may be required to conduct sampling, or propose an alternate approach to testing, to assess devices which are now in a remote access context, due to COVID-19. Testing should be designed not to disrupt normal working through a reduction in available device or excessive bandwidth consumption at choke-points.
- Whilst not a formal 'CHECK' test, the penetration test should be conducted to the level of thoroughness required by CHECK standards.
- Contributes to the overall statistical report (Aim 5)

22. Mobile Device Compliance Test

22.1. Many organisations have now deployed mobile devices on a corporately managed, or BYOD basis. As such, they rely on management solutions to ensure the safety and security of their data and solutions. These management controls need to be configured to manage risk, and need to be effective.

22.2. The scope:

- A limited time exercise.
- Review the mobile device management policies of the test subject against known good practice, reviewing the device management solution in use.
- Highlight potential risks from the current configuration in the context of corporate & BYOD devices.
- Sample a limited number of devices to ensure desired policies are applied. The sample should be representative of the device types in use, to a minimum of variance in operating systems (e.g. IOS, Android). Sampling may need to be remote and 'walk-through' using video calling due to COVID-19.
- Contributes to the overall statistical report (Aim 5)
- **NOTE: this test may be removed from scope or reduced in scope dependent on overall budget constraints, therefore the cost of this element should be included separately as an optional cost, with costing per test subject across the lot.**

What is not in scope

23. It is not feasible to test all devices on a large internal network without extensive time and effort, and the scope of the project does not include this – though funding will take into account test subject size. The scope of internal pen-testing shall be based on the IT Health Check Principles (PSN).

24. Third party suppliers to test subjects, where not covered above, would not be tested – and we acknowledge the risk that sits in this area. Such tests would still need to be commissioned by the local authority in question.

25. After initial testing, neither remediative action, nor testing of the effectiveness of the remediative action is within scope.

Note on testing / tester accreditations and qualifications

26. Whilst the tests are not being commissioned formally under the CHECK scheme, test providers are required to be a member of a relevant professional organisation, and should act in line with NCSC IT Health Check guidance, subject to the scopes described within this document.

Outputs and Data/ Information Sharing

27. Required reports fall into two groups. Outputs per test subject, and outputs per 'lot'. Intended distribution of these reports is listed under 'How the outputs will be used' later in paragraphs 51-53.

28. Data, information and the analysis of information specific to the cyber security of an specific test subject (local authority) is to be shared only with the test-subject in question, the supplier contracted to perform the testing, the LGA.

29. Data, information and the analysis of information specific to the cyber security of a 'lot' is to be shared only with the supplier contracted to perform the testing, the LGA. Specific data contributions to this information or analysis from individual test-subjects will be anonymised.

30. The LGA will own the Intellectual Property Rights to all of the outputs. This will not restrict the test subjects' access to the reports to which they are a subject.

Organisational Reports

31. **(1a) Technical report with (1b) Data Annexe:** Each test subject will receive a technical report which details the vulnerabilities found together with their location. The report should grade the vulnerabilities by severity and propose remediation actions. The report should be in a standard format (e.g. PDF).

32. The Technical report and Data Annexe should take account of the 'statistical requirements' section below, which details items which should be included.

33. The technical report should be accompanied by Data Annexe, which re-states those vulnerabilities in a readily editable format, to enable test subjects to use the data readily within their operations to assign, manage out and close vulnerabilities (e.g. Excel format).

34. **(2) Senior Leadership/Executive Report:** Each test subject will also receive an executive level report. This report, aimed at senior leadership, should detail at a high level the nature and severity of the vulnerabilities discovered within the organisation, how they may be exploited, and the need for co-ordinated action.

Per-Lot Reports

35. For each lot for which the provider is assigned to deliver, the following should be created:

36. **(3a) Lot-Wide commonality report:** An overall summary report in standard format (e.g. PDF), aimed at senior and executive leadership within the sector, detailing major findings and common vulnerabilities. The report should include the test providers' viewpoint on the major gaps in security and security practice discovered, the risks (& level of risk) associated with those gaps, and strategic considerations for remediation within the community. These elements to be written in readily-accessible language, and should not be viewed as a technical report.

37. The provider may add specific advice and guidance for CIOs and CTOs to this report, in a supplemental section, which may contain more technical language.

38. The commonality report should not readily identify specific organisations by name.

39. **(5) Gap Analysis report:** A brief report, providing the testing company's summarised viewpoint on vulnerabilities which would not have been discovered through an individual, 'standard' exercise in this area, such as a Cyber Essentials Plus assessment or IT Health Check.

40. The Gap Analysis report should not readily identify specific organisations by name.

41. **(4) Statistical Report:** A statistical report per-lot is required from this exercise. The report should be presented in an appropriate format and will be accompanied by relevant aggregate base data **(3b)** for further analysis, if such is required. Please refer to 'Statistical Requirements' below.

Statistical Requirements

42. Test suppliers will be required to provide specific details within the individual test subject reports to support their professional output (1a/1b).

43. Additionally, statistical reporting **(4)** and aggregate base data **(3b)** are required per-lot.

44. For both, certain information will need to be collated during the test phase.

45. To avoid undue complexity, and to allow test companies to leverage their individual expertise, we have minimised the initial requirement. Suppliers may choose to innovate beyond these basic requirements.

46. In relation to individual test subject reports, there is a need to provide information which explicitly identifies the organisation to tie specific vulnerabilities to specific systems.

47. In relation to the per-lot aggregate statistical report, and the base statistical data, there is a need to avoid generating excessive security risks through aggregation. As such, these reports should use keying known to the test supplier to identify the impacted organisation (e.g. Org1,Org2 etc.), and should not contain IP address information or host identifiers.

48. Specifics:

    48.1. The supplier shall use a common language across the lot to describe the test scope in which each vulnerability has been discovered. (e.g. End User Devices (PC/LT), Thin Client, External network,Internal Servers,IAAS Hosted Servers,Web Apps)
    48.2. The naming is to enable statistical analysis, and should be considered on that basis.
    48.3. The tester shall allocate, where feasible, a CVE number to each vulnerability found.
    48.4. For each vulnerability discovered, a base CVSS v3 score shall be logged. Where a CVSS v3 score is not available, the tester should calculate a base score or use CVSS v2.
    48.5. It should be feasible to link base CVSS scores to CVE identifiers, where feasible for statistical purposes.
    48.6. For each vulnerability, the tester, working with the test subject, shall agree a level of temporal risk. Standard terms such as 'Informational, Low, Medium, High' may be used in place of full CVSS score calculation.
    48.7. For each vulnerability, the tester shall assign a likely 'root cause' from one of "*Unknown, Unsupported OS, Unsupported App, Failure to Patch (Supported OS/App), Misconfiguration"*. The supplier may choose to add to this list in the interests of clarity.

49. In relation to the statistical report:

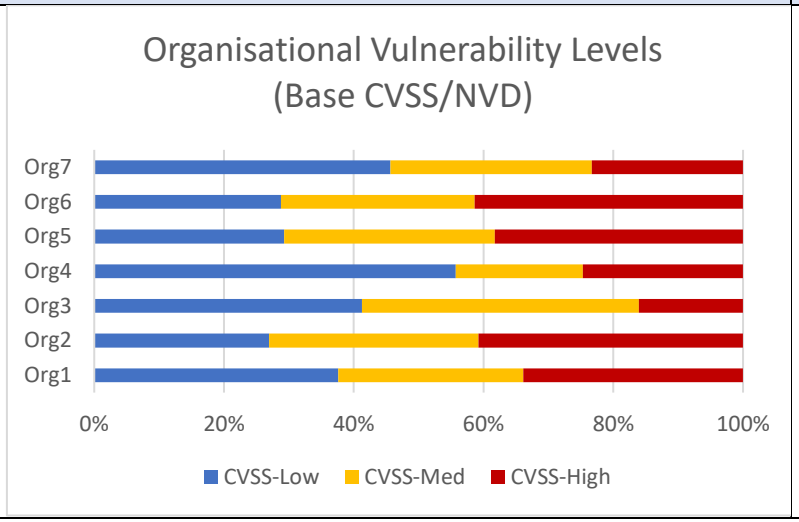
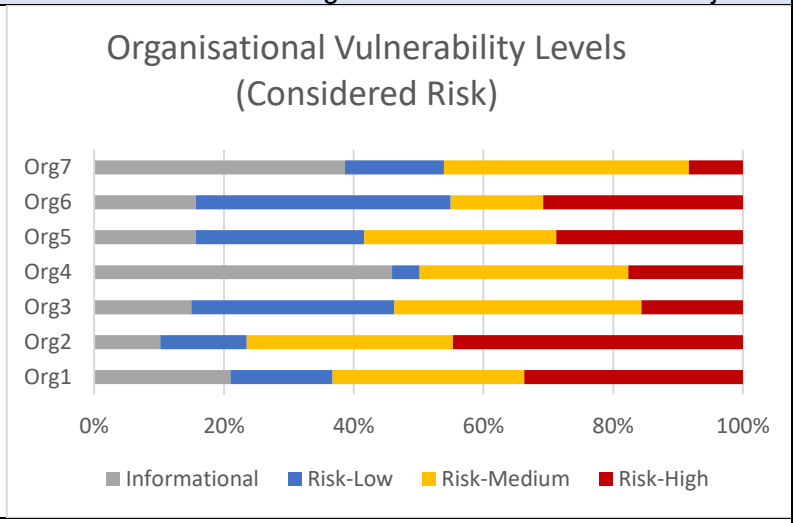
    49.1. The supplier is at liberty to innovate in how the per-lot statistical report is presented, and to use their skills to present information in the most useful and persuasive fashion.
    49.2. As a minimum, however:

49.3. The supplier shall report on the number of hosts (incidence) affected by each level of vulnerability, within each individual test scope (see table under “Examples”).
49.4. The provider shall report on the number of hosts (incidence) affected by each level of temporal risk, within each individual test scope (see table under “Examples”).
49.5. The provider shall report on the incidence of specific vulnerabilities (accompanied by CVE identifiers where feasible), within each individual test scope (see table under ‘Examples’)
49.6. The provider shall report on the root causes of vulnerabilities discovered, as identified within each test scope.

Examples

50. The following examples are provided for informational purposes only, as potential ways of displaying data within the statistical report. The provider is at liberty to innovate in the presentation of statistics, for the sake of clarity and analysis.

50.1. **Report output 1:** Level of vulnerability (raw CVSS score) per test scope per organisation, versus actual level of risk (temporal/assessed)

	Levels of Vulnerability	**Level of vulnerability -** plotted base score CVSS Shows 'raw' scoring before any risk assessment	**Level of vulnerability** - plotted temporal risk level (H,M,L,I) Shows the level of risk agreed between tester and subject.
Context/Scope	End User Devices – PC, Laptop, Thin Client		
	External network	Similar graphical plotting would be performed for each scope.	
	Internal Servers		
	IAAS Hosted Servers		
	Web Applications		

50.2. Example report output 2: Top-10 most common vulnerabilities per test scope by CVE and incidence

End User Devices *(e.g. Followed by the same for external network, internal servers, IAAS, web apps, etc.)*

Incidence	**Description**	**CVE reference**	**Likely Root Cause**
500	Vulnerability Description	CVE-2020-123456	Failure to patch
80	Etc.	Etc.	etc
…	…	…	...

50.3. Example report output 3: Top-50 Highest Ranking vulnerabilities by base CVSS, incidence & CVE

End User Devices *(e.g. Followed by the same for external network, internal servers, IAAS, web apps, etc.)*

Base CVSS score		**Description**	**CVE reference**	**Likely Root Cause**
10.0	25	Vulnerability Description	CVE-2020-123456	Failure to patch
10.0	10	Etc.	Etc.	etc
9.5	80	…	…	...

How the outputs will be used

51. Outputs from the testing work will have immediate impact within the organisations tested, who will benefit from the knowledge of vulnerabilities within their systems and can consider how they will be remedied.

52. In addition to this:

52.1. The LGA will use the information to assist in profiling the sector and make the case for necessary investment in this area.
52.2. The LGA will share information in the approach described in paragraphs 27-30.

53. The table below shows the purpose and intended audience of each output.

Identifier	Output	Purpose	Audience
1(a)	Individual Council Technical Report	To inform IT Practitioners of vulnerabilities identified across their IT infrastructure.	IT Practitioners, LGA
1(b)	Individual Council Technical Report Data Annex	To provide IT Practitioners of vulnerabilities identified across their IT infrastructure in a manipulatable and actionable format.	IT Practitioners
2	Individual Council Senior Leadership Report	To inform senior council leaders, in plain English, of vulnerabilities identified across their IT infrastructure.	Local Authority CEX and other senior leaders
3(a)	'Lot'-wide Commonality Report	To inform national stakeholders, in plain English, of common vulnerabilities identified across councils within each 'lot'	LGA, County Councils Network, District Councils Network, Cabinet Office, Ministry of Housing Communities and Local Government
3(b)	'Lot'-wide Report Data Annex	To provide common vulnerabilities identified across councils within each 'lot' in a manipulatable and actionable format.	LGA, NCSC
4	Statistical Report per 'lot'	To provide a statistical analysis to national stakeholders of common vulnerabilities identified across councils within each 'lot'	LGA, NCSC
5	Gap Analysis Report per 'lot'	To ascertain the vulnerabilities identified by these tests which would not have been found through a single IT Health Check or Cyber Essentials + assessment.	LGA, County Councils Network, District Councils Network, Cabinet Office, Ministry of Housing Communities and Local Government, NCSC

Timings

54. We expect the procurement to conclude in mid-January.

55. A kick off meeting with the supplier/s is scheduled for the 14th/15th January 2021. The work must be completed throughout January, February and March 2021 with the deadline for the outputs being March 31st 2021.

56. LGA colleagues will support the appointed supplier/s to work with the councils within their 'lot/s' to develop a plan for the work to take place within this timescale.

Procurement Timeline

Task	Day	Week	Date
Issue Tender	1	1	4th Dec
Deadline for the submission of clarification questions	11	3	18th Dec
Deadline for response to clarification questions	13-14	4	22nd – 23rd Dec
Deadline for submission of proposals	23	6	5th Jan
Evaluation of proposals	23-28	6/7	12th Jan
Award contract	29+	7	13th Jan
Kick off meeting with suppliers			14th Jan – 15th Jan
Work commences			14th Jan – 31st March

Form of proposal

57. Proposals should be presented by a written document containing the following information

    57.1. A succinct summary of the proposal including clarity on which 'lots' are within the scope of the bid
    57.2. A demonstrable understanding of required outcomes [and sector]

57.3. Your organization's experience of similar projects and [relevant] capability
57.4. Details of the personnel to be involved including their role for this project and their relevant experience
57.5. Arrangements for managing this work and quality assuring outputs, including how you would like to work with the test subject during the project
57.6. A detailed budget / costing. These costs should include reasonable expenses with a clear estimate for expenses included in a separate line. All expenses will need to be in line with the LGA's expenses policy which is included as a document in the tender pack (**Annex B**).

Pricing

The supplier will be reimbursed following completion by the supplier, and sign off from the LGA, of all the required outputs/deliverables for the 'lot' / 'lots' they are delivering.

Evaluation Criteria

58. The below table states how each bid will be scored. A team of LGA colleagues will independently assess and score against the quality criteria below.

59. Price will be scored once as follows:

59.1. Lowest price gets maximum score.
59.2. Highest price gets lowest score.
59.3. Others are scored in relative to how close / far they are to the lowest price via this formula - ((Highest Price – proposal price) / lowest price) *100

Criteria	Sub-criteria	Relative Weighting Percentage
Quality	Suitability of methodology/ approach (maximum score 100)	10%
	Experience in the area/ technical merit (maximum score 100)	10%
	Implementation Timescales (maximum score 100)	30%
	Evidence of understanding the brief (maximum score 100)	10%

Price (maximum score 100)	N/A	40%

59.4. Example:
Based on a bid of £11,000 where the lowest bid was £10,000, and the highest bid was £20,000 (*costs used for illustrative purposes and not intended as a guide)*

Criteria	Sub-criteria	Relative Weighting Percentage	Score	Weighted Score
Quality	Suitability of methodology/ approach (maximum score 100)	10%	30	3
	Experience in the area/ technical merit (maximum score 100)	10%	40	4
	Implementation Timescales (maximum score 100)	30%	90	27
	Evidence of understanding the brief (maximum score 100)	10%	90	9
Price	N/A	40%	90 *Calculated by ((£20000 - £11,000)/£10000)*100)*	36
			Total Score	**79**

Mandatory Requirements

60. Quality Standards

Suppliers shall use a documented quality management system, as part of delivering services under this DPS. The Supplier may be required by a Buyer to comply with specific quality standards set by industry bodies or Government codes of practice.

61. Security Requirements

The Supplier shall at all times during the DPS Contract Period and during the term of any Order Contract comply with the Buyer's contracted security requirements. The Supplier will ensure controls and measures are in place to protect data handled, processed or stored as part of delivering the Services in accordance with Clause 14 of the Core Terms.

The Supplier shall comply with the applicable requirements set out in the Cabinet Office's Security Policy Framework. Information about the framework can be found at:https://www.gov.uk/government/publications/security-policy-framework

The Supplier shall ensure that staff has security clearance to a minimum level: Baseline Personnel Security standard (BPSS). Should a Buyer require a higher level of security clearance this will be made clear in the Order Procedure.

62. Environmental Standards

Where applicable, the Supplier shall ensure that all Electric and Electronic Equipment (EEE) used or disposed of as part of delivery of the Services, complies with Restriction of Hazardous Substances (RoHs), WEEE regulations, or equivalent. Full details can be found via the following links: http://www.hse.gov.uk/waste/waste-electrical.htm

63. Complying with future government requirements and standards

The Supplier shall comply with relevant future Government requirements and standards in accordance with any Government guidance issued during the DPS Contract Period and as developed and updated, from time to time.

64. Staff and Contractors

Where appropriate the Supplier shall ensure that appropriate roles and grades of staff will be assigned to the Services in accordance with NCSC - defined experience levels, Skills Framework for the Information Age (SFIA), or other equivalent grading structures used by the cyber security industry for personnel providing the Services offered under this DPS.

65. Social Value

The Supplier shall identify Social Value options which are appropriate to Buyers at Order Contract award stage in accordance with the Buyer's requirements communicated as part of their Order Procedure.

The Supplier shall complete annual Corporate Social Responsibility (CSR) assessments upon request from Buyers where specified as part of their Order Contract Obligations.

For more information on Social Value please see the following link: https://www.gov.uk/government/publications/social-value-act-introductory-guide

Annex A – Council Information Profiles (anonymised) by 'lot'

About the profiles

1. The following profiles have been provided, through surveying in Q3/Q4 2020, by the organisations who will be partaking in the exercise. The information is provided to assist in your consideration of costs and is not guaranteed to be complete or accurate at the time of testing.

Lot 1 – 18 District Councils

End User Devices				Scale		Platform as a Service (PAAS)
Type	**Number of PCs**	**Number of Laptops**	**Laptops % used for remote access**	**Number of servers on your network**	**Number of servers in the cloud**	**Web app hosting platforms**
D	600	250	100%	250	0	Azure
D	800 (reducing to 100)	200 (increasing to 800)	100%	220	0	Azure
D	100	500	95%	180	0	Azure
D	250 (majority thin client)	250	100%	160	0	None
D	100	500	100%	150	150	Azure
D	100	200	99%	130	0	None
D	500	300	99%	125	0	None
D	62	346	100%	109	59	Azure
D	0	250	99%	80	0	None
D	10	600	85%	70	5	AWS Azure Salesforce
D	600	370	100%	1	10	None
D	10	600	95%	0	44	Azure
D	Not provided					

D	
D	
D	
D	
D	

Lot 2 – 8 Unitary Authorities

End User Devices				Scale		Platform as a Service (PAAS)
Type	**Number of PCs**	**Number of Laptops**	**Laptops % used for remote access**	**Number of servers on your network**	**Number of servers in the cloud**	**Web app hosting platforms**
UA	500	2200	68%	380	0	Azure
UA	3400	2386	100%	334	0	Azure
UA	400	2500	60%	290	3	Azure
UA	400	2600	95%	250	0	None
UA	1700	800	95%	150	0	None
UA	200	4400	85%	11100	27	Azure (x10)
UA	Not provided					
UA						

Lot 3 – 3 London Boroughs

End User Devices				Scale		Platform as a Service (PAAS)
Type	**Number of PCs**	**Number of Laptops**	**Laptops % used for**	**Number of servers on your network**	**Number of servers in the cloud**	**Web app hosting platforms**

			remote access			
LON	100	3300	100%	740	11	Azure
LON	100	1900	99%	170	45	Azure & AWS
LON	300	2200	100%	40	150	Azure

Lot 4 – 3 County Councils

End User Devices				Scale		Platform as a Service (PAAS)
Type	**Number of PCs**	**Number of Laptops**	**Laptops % used for remote access**	**Number of servers on your network**	**Number of servers in the cloud**	**Where you have web apps, which platforms have you used to host the service?**
CC	12087	18603	100%	3306	0	SAP
CC	150	6350	100%	450	50	Azure
CC	450 desktops 1050 thin client	3500	90%	350	0	Azure