

Statement of Requirement (SoR)

Reference Number	RQ0000038652
Version Number	1.0
Date	20/09/2023

1.	Requirement
1.1	Title
	UWG IT Health Check
1.2	Summary
	A CHECK approved IT Health Check on the UK AR&A system network in Underwater Group (UWG), according to the scoping meeting. This would preferably start before December 2023 and the deliverable includes two reports and a remediation spreadsheet back to UWG, with analytical feedback on the risks, CVSS scores and findings.
1.3	Background
	The UK AR&A computer system in UWG is a system that takes data from missions, processes it and allows users to write reports for customers. It also allows training courses to be written on it. The system is highly classified and as such requires an IT Health Check every year. We are required to go to Crown Commercial Services who source contractors assured by the National Cyber Security Centre (NCSC) with our IT Health Check requirement.
1.4	Requirement

Network scan (TCP/UDP ports)

Scan all servers and a selection of workstations for up to date patches


Check select applications for vulnerabilities (discussed during scoping).

Build and configuration review on representative servers/workstations.

Password analysis.

Show any exploits found, consult IT Admin team before exploiting due to live data on the system.

Provide a report on completion detailing vulnerabilities and recommendations.

Provide an  executive summary with findings and CVSS scoring.


These are the general mandatory requirements – specifics are usually discussed at the scoping meeting.

Milestone	Description	Timeframe
Initial Scoping Meeting	An initial scoping meeting before testing begins, involving representatives from an assured NCSC provider, UWG Admin, ITSO and Facility Manager. This is to discuss the ITHC scope and address any questions.	Usually a month prior to testing to ensure hardware delivery and checks can be completed within time.
Testing	Two NCSC assured pen testers testing as agreed during the scoping meeting.	4 days
Report Writing	Pen testers producing reports outlining their findings whilst adding CVSS scoring and remediation advice.	2 days
Report Breakdown	Pen testers reviewing the report findings and remediation actions with UWG.	2 days
Remediation Actions	UWG begin to address the remediation actions disclosed within the reports.	On receipt of the final report(s) and remediation file being delivered to UWG.

Work will be monitored on whether the areas defined in the scoping meeting have been tested to the degree agreed.

	<p>Approach, such as which kinds of tests are done in which order are defined in the scoping meeting.</p> <p>We usually have two staff working eight days, but this is confirmed after the scoping meeting. Four days IT Health Check, one-two days report writing and one-two days running through the report understanding the tasking and outcome.</p> <p>The delivered tasking for the IT Health Check must be conducted on consecutive days.</p> <p>The staff are required to have a DV clearance.</p> <p>The staff are assured by NCSC so will meet NCSC's (skills and other) criteria for this work such as CHECK approved.</p> <p>IT Health Check provider to supply appropriate testing software and report writing software on two UEFI bootable SATA SSDs sent to UWG for registering and testing two weeks prior to the IT Health Check start date. Due to the classification, these media will remain on-site and are not returnable.</p>
1.5	Options or follow on work
	Not applicable

1.6 Deliverables & Intellectual Property Rights (IPR)							
Ref.	Title	Due by	Format	TRL *	Expected classification (subject to change)	What information is required in the deliverable	IPR DEFCON/ Condition
D – 1	Report detailed findings of tests with CVSS scoring. Detail and format to be agreed at scoping meeting. Report to be understood following ITHC.	As soon as the ITHC has been completed whilst on-site.	PDF Format	n/a		Report findings of IT Health Check with recommendations on protecting against those findings, including links that support this.	Cyber Security Services 3 DSP terms apply
D - 2	Executive Summary reporting giving an overview of the findings/risks, including numbers and charts.	As soon as the ITHC has been completed whilst on-site.	PDF Format	N/A		An executive summary of the IT Health Check findings giving an overview of the risks, including charts.	Cyber Security Services 3 DSP terms apply

D - 3	Remediation spreadsheet with all the findings, including CVSS scoring and remediation actions.	As soon as the ITHC has been completed whilst on-site.	XLSX Format	N/A		A remediation spreadsheet	Cyber Security Services 3 DSP terms apply
-------	--	--	-------------	-----	--	---------------------------	--

***Technology Readiness Level required**

1.7	Standard Deliverable Acceptance Criteria
	<p>All reports included as deliverables under the contract must comply with the Defence Research Reports Specification (DRRS), which defines the requirements for the presentation, format and production of scientific and technical reports prepared for MoD.</p> <p>All deliverables shall be supplied in accordance with the Security Aspects Letter for this task.</p> <p>All deliverable documents and reports shall be produced using Microsoft Office 2016 applications.</p> <p>The IT Health Check must be conducted by CHECK approved providers.</p>
1.8	Specific Deliverable Acceptance Criteria
	<p>An executive summary at a lower classification with the risks and findings at a high-level.</p>

2.	Quality Control and Assurance
2.1	Quality Control and Quality Assurance processes and standards that must be met by the contractor
	<p><input type="checkbox"/> ISO9001 (Quality Management Systems)</p> <p><input type="checkbox"/> ISO14001 (Environment Management Systems)</p> <p><input type="checkbox"/> ISO12207 (Systems and software engineering — software life cycle)</p> <p><input checked="" type="checkbox"/> TickITPlus (Integrated approach to software and IT development)</p> <p><input type="checkbox"/> Other: (Please specify below)</p>
2.2	Safety, Environmental, Social, Ethical, Regulatory or Legislative aspects of the requirement
	Not applicable

3.	Security	
3.1	Highest security classification	
	Of the work	[REDACTED]
	Of the Deliverables/ Output	[REDACTED]
3.2	Security Aspects Letter (SAL)	
	Yes If yes, please see SAL reference- RQ0000038652	
3.3	Cyber Risk Level	
	[REDACTED]	
3.4	Cyber Risk Assessment (RA) Reference	
	[REDACTED] If stated, this must be completed by the contractor before a contract can be awarded. In accordance with the Supplier Cyber Protection Risk Assessment (RA) Workflow please complete the Cyber Risk Assessment available at https://www.gov.uk/guidance/supplier-cyber-protection-service	

4.	Government Furnished Assets (GFA)				
GFA to be Issued - Yes					
GFA No.	Unique Identifier/ Serial No	Description:	Available Date	Issued by	Return Date or Disposal Date (T0+)

GFE-1	ISAx	Workstation	During Contract.	UWG	End of Contract.
GFE-2	ISAx	Workstation	During Contract.	UWG	End of Contract.
GFF-1	N/A	Desk, chairs.	During Contract.	UWG	End of Contract.

5.	Proposal Evaluation criteria
5.1	Technical Evaluation Criteria

Technical Criteria 60%

Proposals will be assessed by the Dstl Project Technical Authority and Commercial Authority using the following criteria and weighting.

This requirement will be competed and awarded on the basis of best Weighted Value for Money Index. The winning tender will be subject to available funding. DSTL reserves the right to fail a tender exceeding the unrevealed limit on grounds of unaffordability.

Technical criteria 60%
Cost 40%

Tenders will be technically evaluated using the criteria supplied in the following table. The maximum technical score is 30, the minimum score is 0.

Descriptions of the criteria and what constitutes an excellent to poor response are provided. A score of 0 or 1 in any of the criteria will result in the tender being assessed as technically non-compliant and will be excluded from the competition.

The three technical criteria are equally weighted.

Technical Category		Max Score (0-10)
Describe how would you ensure that vulnerability assessments are carried out to an acceptable standard without affecting a live environment?		10
Describe how your final report will meet the objectives of the requirement (e.g. structure, length, audience, etc.).		10
How do you structure your approach whilst penetrating a network in a layered environment?		10
Mark	Criteria	
0 – Unacceptable or no answer	Has demonstrated inadequate experience or provided inadequate supporting evidence which gives no confidence of the Potential Tenderer's competence and an unacceptably high level of risk to the project	

5. Proposal Evaluation criteria									
5.1 Technical Evaluation Criteria									
	<table> <tr> <td>1 – Poor response with Very High risk</td><td>Has demonstrated narrow experience or provided minimal supporting evidence which gives low confidence of the Potential Tenderer's competence and a very high level of risk to the project.</td></tr> <tr> <td>4 – Satisfactory with Medium to High risk</td><td>Has demonstrated some experience and provided adequate supporting evidence which gives some confidence of the Potential Tenderer's competence and a low to medium level of risk to the project.</td></tr> <tr> <td>7 – Good with Low to Medium risk</td><td>Has demonstrated broad experience and provided adequate supporting evidence which gives confidence of the Potential Tenderer's competence and a low to medium level of risk to the project.</td></tr> <tr> <td>10 – Excellent with Very Low risk</td><td>Has demonstrated considerable and detailed experience and provided sound and relevant supporting evidence which gives high confidence of the Potential Tenderer's competence and a very low level of risk to the project.</td></tr> </table>	1 – Poor response with Very High risk	Has demonstrated narrow experience or provided minimal supporting evidence which gives low confidence of the Potential Tenderer's competence and a very high level of risk to the project.	4 – Satisfactory with Medium to High risk	Has demonstrated some experience and provided adequate supporting evidence which gives some confidence of the Potential Tenderer's competence and a low to medium level of risk to the project.	7 – Good with Low to Medium risk	Has demonstrated broad experience and provided adequate supporting evidence which gives confidence of the Potential Tenderer's competence and a low to medium level of risk to the project.	10 – Excellent with Very Low risk	Has demonstrated considerable and detailed experience and provided sound and relevant supporting evidence which gives high confidence of the Potential Tenderer's competence and a very low level of risk to the project.
1 – Poor response with Very High risk	Has demonstrated narrow experience or provided minimal supporting evidence which gives low confidence of the Potential Tenderer's competence and a very high level of risk to the project.								
4 – Satisfactory with Medium to High risk	Has demonstrated some experience and provided adequate supporting evidence which gives some confidence of the Potential Tenderer's competence and a low to medium level of risk to the project.								
7 – Good with Low to Medium risk	Has demonstrated broad experience and provided adequate supporting evidence which gives confidence of the Potential Tenderer's competence and a low to medium level of risk to the project.								
10 – Excellent with Very Low risk	Has demonstrated considerable and detailed experience and provided sound and relevant supporting evidence which gives high confidence of the Potential Tenderer's competence and a very low level of risk to the project.								
5.2 Commercial Evaluation Criteria									

Element	Requirement	Weighting
C1	Compliance with the Cyber Security Services 3 terms and conditions	Pass/Fail
C2	Please submit your full firm price breakdown for all costs to be incurred, including: <ul style="list-style-type: none"> • Labour costs • Travel & Subsistence costs • Any Materials costs • Any Facility costs • Any Sub-Contractor costs • Any other costs 	Pass/Fail
Mark	Definition	
Pass	Fully meets the Authority's requirement. Provision and acceptance of the sub-criteria information in the format requested, which is clear, unambiguous and transparent.	
Fail	Unacceptable/Nil Return. Tenderer did not respond to the question or the response wholly failed to demonstrate an ability to meet the sub-criteria requirement. Any proposal marked as a Fail will be excluded from the competition.	

Calculation of total score

The below worked example shows how the tender total score will be calculated.

The winning tender is the one with the highest weighted value for money index. In the event of a tie-break between suppliers for the highest score, the tie supplier with the highest technical mark will be awarded the contract.

Weighted Value for Money Index example

The overall tender score is calculated as follows:

$$\frac{\text{Technical Score } 60/40}{\text{Cost}}$$

Tender	Technical Score	Cost (£)	Weighted VFM Index	Rank
A	$21^{60/40} = 96.23$	40000	0.00241	2 nd
B	$27^{60/40} = 140.30$	50000	0.00281	1 st
C	$18^{60/40} = 76.37$	45000	0.00170	3 rd

Weighted VFM is rounded to three significant figures