

## Statement of Requirement (SoR)

Reference Number	RQ0000071775
Version Number	1.0
Date	03/03/2025

1.	Requirement
1.1	Title
	UWG IT Health Check 2025
1.2	Summary
	A CHECK approved IT Health Check on the UK Acoustic Replay & Analysis System (UKAR&AS) network in Underwater Group (UWG), according to the scoping meeting. The deliverables includes two reports and a remediation spreadsheet back to UWG, with analytical feedback on the risks, Common Vulnerability Scoring System (CVSS) scores and findings.
1.3	Background
	The UKAR&A computer system in UWG is primarily a data processing system, and due to its classification 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

An internal IT Health Check and penetration testing assessment that adheres to the NCSC CHECK requirements, delivered by an accredited CHECK Team, including two DV-Cleared CHECK Team Leaders. The two CHECK Team Leaders will both be certified within the Infrastructure discipline as a minimum, with at least one also holding certification in the Application discipline.

Testing will include, but not be limited to, the following:

- Network scanning to identify exposed services operating on Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports.
- Vulnerability scanning and patch scanning of all servers and a selection of workstations for up-to-date patches.
- Assessment of selected applications for exploitable vulnerabilities (to be discussed during scoping).
- Build and configuration reviews of representative servers/workstations.
- Password analysis of all servers and representative workstations. This will also include relevant network devices and applications where applicable.
- Demonstration of exploitation of identified vulnerabilities where system integrity and availability will not be impacted. Prior to any exploitation attempts, plans and related risks will be discussed with IT Admin team, with exploitation on live systems performed only with express permission.

All testing and meetings will be conducted at Portsdown West. Specific dates are TBD but possible windows for the on-site element of the work are between June 9<sup>th</sup>-August 22<sup>nd</sup> 2025 or between Oct 19<sup>th</sup>-Nov 28<sup>th</sup> 2025, with **Nov 28<sup>th</sup> 2025 being the absolute deadline** for completion of any on-site work. Suppliers will need to confirm their availability based on the above dates.

Reporting should consist of a detailed technical report covering the areas above, including:


- An executive summary with tailored risk management guidance; and
- Detailed technical breakdown including evidence and remediation advice where appropriate.
- CVSS 3.1 base scores where applicable

These are the general mandatory requirements – specifics will be 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 & Presentation	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.
<p>Work will be monitored on whether the areas defined in the scoping meeting have been tested to the degree agreed.</p> <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. The typical breakdown is 4-5 days of IT Health Check, 2 days report writing and 1-2 days presenting the reports 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 Unified Extensible Firmware Interface (UEFI) bootable Serial AT Attached (SATA) Solid State Drives (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>			
<b>1.5</b>	<b>Options or follow on work</b>		
	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	Scoping Meeting	TBD (before start of on-site testing)	In Person Meeting	n/a	[REDACTED]	Discussion between Secure Network Team to correlate requirements with supplier working methodology and establish the details of the subsequent deliverables.	As per Cyber Security Services 3 RM3764iii-DPS-Core-Terms
D-2	Report detailed findings of tests with CVSS scoring. Detail and format to be agreed at scoping meeting. Report to be understood following ITHC.	TBD (Est. 4 weeks after on-site testing completes.)	PDF Format	n/a	[REDACTED]	Report findings of IT Health Check with recommendations on protecting against those findings, including links that support this.	As per Cyber Security Services 3 RM3764iii-DPS-Core-Terms

D-3	Executive Summary reporting giving an overview of the findings/risks, including numbers and charts.	TBD (Est. 4 weeks after on-site testing completes.)	PDF Format	n/a		An executive summary of the IT Health Check findings giving an overview of the risks, including charts.	As per Cyber Security Services 3 RM3764iii-DPS-Core-Terms
D-4	Remediation spreadsheet with all the findings, including CVSS scoring and remediation actions.	TBD (Est. 4 weeks after on-site testing completes.)	XLSX Format	n/a		A remediation spreadsheet.	As per Cyber Security Services 3 RM3764iii-DPS-Core-Terms

**\*Technology Readiness Level required**

<b>1.7</b>	<b>Standard Deliverable Acceptance Criteria</b>
	<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>
<b>1.8</b>	<b>Specific Deliverable Acceptance Criteria</b>
	<p>An executive summary at a lower classification with the risks and findings at a high-level.</p>

<b>2.</b>	<b>Quality Control and Assurance</b>
<b>2.1</b>	<b>Quality Control and Quality Assurance processes and standards that must be met by the contractor</b>
	<p><input type="checkbox"/> <b>ISO9001</b> (Quality Management Systems)</p> <p><input type="checkbox"/> <b>ISO14001</b> (Environment Management Systems)</p> <p><input type="checkbox"/> <b>ISO12207</b> (Systems and software engineering — software life cycle)</p> <p><input checked="" type="checkbox"/> <b>TickITPlus</b> (Integrated approach to software and IT development)</p> <p><input type="checkbox"/> <b>Other:</b> (Please specify below)</p>
<b>2.2</b>	<b>Safety, Environmental, Social, Ethical, Regulatory or Legislative aspects of the requirement</b>
	<p>Supplier will be responsible for ensuring they follow all relevant legislation whilst carrying out the contract.</p>

<b>3.</b>	<b>Security</b>	
<b>3.1</b>	<b>Highest security classification</b>	
	<b>Of the work</b>	[REDACTED]
	<b>Of the Deliverables/ Output</b>	[REDACTED]
<b>3.2</b>	<b>Security Aspects Letter (SAL)</b>	
	Yes  If yes, please see SAL reference- [REDACTED]	
<b>3.3</b>	<b>Cyber Risk Profile</b>	
	High	
<b>3.4</b>	<b>Cyber Risk Assessment Reference</b>	
	[REDACTED]  In accordance with the <a href="#">Defence Cyber Protection Partnership</a> and DefCon 658 a Supplier Assurance Questionnaire must be completed by the contractor before a contract can be awarded where a Cyber Risk Assessment Reference (RAR) has been provided.	

<b>4.</b>	<b>Government Furnished Assets (GFA)</b>				
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	Return at end of contract
GFE-2	ISAx	Workstation	During contract	UWG	Return at end of contract
GFF-1	n/a	Desk, chairs etc	During contract	UWG	Return at end of contract



5.	<b>Proposal Evaluation criteria</b>								
5.1	<b>Technical Evaluation Criteria</b>								
	<p><b>Technical Criteria 60%</b></p> <p>Proposals will be assessed by the Dstl Project Technical Authority and Commercial Authority using the following criteria and weighting.</p> <p>This requirement will be competed and awarded on the basis of best Weighted Value for Money Index. The technically and commercially complaint bid with the highest weighted value for money index will be the winner. 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.</p> <p>Technical criteria 60%</p> <p>Cost 40%</p> <p>Tenders will be technically evaluated using the criteria supplied in the following table. The maximum technical score is 30, the minimum score is 0.</p> <p>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.</p> <p>The three technical criteria are equally weighted.</p> <table border="1"> <thead> <tr> <th>Technical Category</th><th>Max Score (0-10)</th></tr> </thead> <tbody> <tr> <td>Describe how would you ensure that vulnerability assessments are carried out to an acceptable standard without affecting a live environment?</td><td>10</td></tr> <tr> <td>Describe how your final report will meet the objectives of the requirement (e.g. structure, length, audience, etc.).</td><td>10</td></tr> <tr> <td>How do you structure your approach whilst penetrating a network in a layered environment?</td><td>10</td></tr> </tbody> </table>	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
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	
	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	<p>Please submit your full firm price breakdown for all costs to be incurred, including:</p> <ul style="list-style-type: none"><li>• Labour costs</li><li>• Travel &amp; Subsistence costs</li><li>• Any Materials costs</li><li>• Any Facility costs</li><li>• Any Sub-Contractor costs</li><li>• Any other costs</li></ul>	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.  <b>Any proposal marked as a Fail will be excluded from the competition.</b>

**Calculation of total score**

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

A fail against any of the commercial criteria will result in the tender being assessed as commercially non-compliant and will be excluded from the competition.

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 tied supplier with the highest technical mark will be awarded the contract.

The overall tender score is calculated as follows:

Technical Score <sup>60/40</sup>

Cost

**Weighted Value for Money Index example**

Tender	Technical Score	Cost (£k)	Weighted VFM Index	Rank
A	$21^{60/40} = 96.23$	18	5.35	2 <sup>nd</sup>
B	$27^{60/40} = 140.30$	25	5.61	1 <sup>st</sup>
C	$18^{60/40} = 76.37$	22	3.47	3 <sup>rd</sup>
Weighted VFM is rounded to three significant figures				