Driver & Vehicle Licensing Agency

Statement of Requirements – Provision of Third Party Assurance Under the GovAssure Scheme

Contents page

1. Purpose

1.1. GovAssure will enable the Driver and Vehicle Licensing Agency (DVLA) to accurately assess its level of cyber assurance for their critical systems against a proportionate CAF threat profile, highlighting priority areas for improvement.

2. Background to the contracting authority

2.1 DVLA is an Executive Agency of the Department for Transport (DfT), based in Swansea. DVLA's primary aims are to facilitate road safety and general law enforcement by maintaining accurate registers of drivers and vehicle keepers to collect Vehicle Excise Duty (VED).

3. Background to requirement/overview of requirement

3.1 GovAssure is the new cyber security assurance approach for government that will replace the cyber security element of the Departmental Security Health Check (DSHC) from April 2023.

3.2 GovAssure is designed for OFFICAL systems and does not currently apply to systems processing data classified as SECRET or above. Higher classification systems will be considered at a later date. GovAssure will apply to government sector Critical National Infrastructure (CNI), bringing them under a common assurance process for cyber.

3.3 Organisations that handle government data and information, such as DVLA are required to assess their cyber resilience against the appropriate government profile under the NCSC's Cyber Assessment Framework (CAF), in accordance with the guidance and policy under the HMG GovAssure cyber assurance regime and Government Cyber Security Policy Handbook. GovAssure will enable DVLA to create and implement a targeted improvement plan to prioritise and address the security challenges to achieving the outcomes of their government profile.

3.4 GovAssure is a key enabler to improve HM Government's cyber security posture and achieve the aim and vision set out in the Government Cyber Security Strategy, published in January 2022. The findings from DVLA's GovAssure review will help identify key remediations needed to be implemented to improve the cyber security resilience of DVLA, prioritise cyber investment decisions and provide DVLA senior stakeholders and Government Security Group with the necessary assurances.

4. Definitions

Expression or Acronym	Definition
NCSC	National Cyber Security Centre
GSG	Government Security Group
CAF	Cyber Assessment Framework
WebCAF	Online platform where departments will complete their self-assessment of systems against the relevant government profile under the NCSC's CAF.

5. Scope of requirement

5.1 Please see below a list of in scope requirements:

5.1.1 The following is included in scope for the supplier:

5.1.1.1 Attending a planning/start up meeting via Microsoft Teams between DVLA to set out review approach, ways of working and review logistics;

5.1.1.2 The completion of an Independent assessment of Driver and Vehicle Licensing Agency self-assessments, on WebCAF, against the appropriate Government profile against the CAF;

5.1.1.3 Access to the evidence and information referenced in Driver and Vehicle Licensing Agency self-assessment;

5.1.1.5 The development of a final technical report, based on the Independent Assessment of DVLA's self-assessment on WebCAF, agreed between the supplier, DVLA and Government Security Group.

5.1.2 The following is not in scope for the supplier:

5.1.2.1 Providing cyber implementation services to DVLA's self-assessments, on WebCAF;

5.1.2.2 The development of the targeted improvement plan;

5.1.2.3 Conducting a GovAssure review on further systems out of the scope for DVLA GovAssure review;

5.1.2.4 To discuss or agree what CAF profile systems going through GovAssure will be measured against;

5.1.2.5 To provide non-data driven decisions or speculative recommendations on what Driver and Vehicle Licensing Agency should do to mitigate cyber risk.

6. The requirement

6.1 DVLA wishes to procure a supplier to conduct an independent assurance review of DVLA's self-assessed assessment of three (3) systems going through GovAssure returns against the National Cyber Security Centre's Cyber Assessment Framework.

6.2 Following DVLA completing a self-assessment of three (3) of systems going through GovAssure against an appropriate government profile (baseline or enhanced) under the National Cyber Security Centre's Cyber Assessment Framework, a supplier will conduct an assessment of the department's systems in scope, assessing the completed self-assessment and provided evidence to author a final report stating whether DVLA meets the assigned government profile against the systems in scope.

6.3 Before the assessment begins, the supplier will hold a planning/start up meeting via Microsoft Teams with DVLA and Government Security Group to outline review timelines and logistics. In this meeting DVLA will present their completed GovAssure Scoping Document. The supplier will then work with DVLA throughout the review period. The supplier will then author a final technical report, with a final version agreed by DVLA and Government Security Group.

6.4 The supplier will have secure access to the evidence and information presented by Driver and Vehicle Licensing Agency in their self-assessment of the Cyber Assessment Framework. DVLA will decide the most appropriate way of sharing information with suppliers. DVLA data and information must not sit on the supplier's network or devices.

6.5 The supplier should be willing to work virtually. There is a requirement for the supplier to attend DVLA, Longview Road, Morriston Swansea, SA6 7JL to securely collect and return laptops (which may be met by the use of an agreed secure courier).

6.6 The final deliverable will be a final technical report for DVLA providing an independent assessment of whether DVLA meets the relevant Government profile under the National Cyber Security Centre's Cyber Assessment Framework.

6.7 The supplier will only use the template and WebCAF provided by Government Security Group when completing the independent assurance review and authoring the final technical report.

6.8 All members from the supplier's team working on DVLA GovAssure review will hold SC clearance.

6.9 For each GovAssure Independent Assurance Review that organisations bid for, there must be a **named authority.** The named authority is responsible for signing-off the audit on behalf of the organisation carrying out the audit.

6.10 This individual (named authority) should either be a Head Consultant for Risk Management or Audit & Review.

6.11 The named authority does not necessarily need to perform parts of the assessment, but should have oversight throughout the review. In signing off any of the outputs from the review they are taking responsibility on behalf of their organisation that the audit has been conducted to satisfactory standards (both company and Cabinet Office) and they will act as a point of escalation if any issues or questions subsequently arise.

6.12 The named authority for the supplier will have experience of working within HM Government (this includes the wider public sector). DVLA will require customer references/ contract examples from the supplier.

6.13 In the interests of transparency, the buyer must declare any potential conflicts of interest when it comes to providing assurance on a specific government system e.g. they may have been involved in the design of the system or CHECK pen testing previously, or involved in architectural design reviews. This won't necessarily preclude that company from bidding for the work, but failure to declare any interests could preclude them from bidding for future GovAssure work. Suppliers will be required to complete a conflict of interest form as part of their submission.

7. Key milestones and deliverables

7.1 The following Contract milestones/deliverables shall apply:

Milestone/Deliverable	Description	Timeframe or Delivery Date

Preparation for assurance reviews	A planning/start up meeting between the supplier and DVLA will take place to set out the approach for the Independent Assurance Review, logistics and ways of working.	1 hour
Project Initiation	Collection of Laptops, setup of WebCaf access and access to evidence	1 day
Conduct assurance review	The supplier will conduct the Independent Assurance Review, looking at the WebCAF submissions for each system in scope by DVLA. It is advised that suppliers follow the review methodology as outlined in the GovAssure Assurance Reviewer Training Session that they must have attended. The supplier must comply with the direction in the document GovAssure: Detailed Guidance for Independent Assurance Reviewers This will include assessing the evidence that DVLA have provided and conducting interviews with key stakeholders.	[It is anticipated that this initial assessment of evidence against the self-assessment will take 4 +/- 2 days by an assessment team for each system, depending on: • System level • System type and complexity • System dependencies and use of 3rd party service evidence • Quality of evidence • Assessor team composition
Supplier submission on WebCAF	The supplier will complete a WebCAF submission for each system (referred to as a ***GovAssure WebCAF External Assessment System Report***) indicating whether DVLA meets the Government profile each system has been assigned to.	

Supplier author's draft final report	The supplier will author a draft of the final report referred to as the ***Independent Assurance Review Report***	[This is likely to take 5 days +/- 2 days, during which time the content of the report is prepared.]
Agree final report	The supplier will share the final report with DVLA and Government Security Group. Arbitration may take place if not all parties agree to the final report.	[Once the assessment is done, then the timeframe for arbitration and presentation of the report is probably 2 +/- 1 days, but will depend on: ● The time required for the subject department to review findings and have their own internal discussions, ● The number of CAF points for arbitration ● The practicalities of getting the required personnel together (or made available) for the arbitration process.]
Project closure	Secure return of laptops	1 day

8. Management information/reporting

8.1 The supplier is expected to use the material the Government Security Group has developed to present final review findings to the buyer. GSG will provide this to DVLA and supplier. The government organisation should provide this to the supplier by downloading the relevant guidance from https://www.security.gov.uk/guidance/govassure/

8.2 The Supplier will utilise laptops provided by DVLA (for which the supplier must arrange secure collection and return). Access to DVLA WebCAF data set will be provided, as will remote access to DVLA IT in so far as that may be required to assess evidence. The supplier must ensure that appropriate security is provided for the laptops and credentials provided, ensuring that no person without authorisation obtains access.

8.3 The supplier must ensure that data provided by DVLA as part of this exercise is not stored on any IT other than that provided for the purpose. In the event that any data or notes related to this activity do for any reason come to be on another system this must be securely erased.

9. Volumes

9.1 The supplier is expected to conduct three (3) system assurance reviews for Driver and Vehicle Licensing Agency

9.2 The GovAssure review will be of three (3) of DVLA's IT systems. Based on discussions with Government Security Group one of the three (3) systems to be reviewed is of moderate complexity, the other two (2) systems are of higher complexity. In addition to the WebCAF entries DVLA will endeavouring to provide the minimum necessary documentation to evidence the statements made in the WebCAF self-assessment so as not to increase the amount of effort required to assess the evidence.

9.3 DVLA is working to ensure the volume of evidence is kept to a minimum consistent with substantiating the self-assessment statements.

10. Continuous improvement

10.1 DVLA will not require assistance from the Supplier with any lessons learned or continuous improvement activity in relation to GovAssure

11. Quality

11.1 Suppliers will adhere to the standards set forth by Government Security Group. Government Security Group may conduct some quality assurance over the supplier, so the supplier should be willing to participate in this process if required. Government Security Group will be managing and keeping a record of the overall quality of independent assurance reviews.

11.2 Suppliers must meet the stated accreditation / assurance requirements to carry out a GovAssure review.

11.3 The named authority for the supplier must evidence that they have attended the GovAssure Reviewer Training programme delivered by the NCSC and GSG.

The minimum standards for each GovAssure package are detailed below (Guidance-Government Organisations can select the GovAssure package they wish to include within the statement of requirements).

NCSC GovAssure
To be eligible to select 'GovAssure' through the NCSC Assured Route, suppliers must already be members of the two NCSC Assurance schemes as detailed below:

Assured Consultancy Risk Management **OR**	**AND**	Assured Consultancy Security Architecture **OR**

Assured Consultancy Audit & Review		CHECK Penetration Testing

Non-NCSC Assured GovAssure
To be eligible to select 'GovAssure' through the Non-NCSC Assured Route, suppliers must meet the below criteria:

Overview requirements for a supplier to be on GovAssure	● Professional indemnity insurance ● Management of the use of contractors ● Staff vetting - minimum of one person SC cleared for the review team members ● Complaint handling ● Data management & security ● Cyber Essentials plus certification and information security policies and processes to handle HMG information for the system on which all information relating to GovAssure work is held ● Willingness to use HMG IT equipment
Cyber audit and risk management	**One of**: ● ISO27001 Lead auditor ● ISACA - Certified Information Security Auditor (CISA)
Technical Cyber Security Expert	**One of:** ● CREST Certified Penetration Tester ● CREST Certified Infrastructure Tester ● CREST Certified Web Applications Tester ● CERT Certified Simulated Attack Specialist ● CREST Certified Simulated Attack Manager ● CREST Certified Intrusion Analyst ● Cyber Scheme Team Leader (CSTL) ● TigerScheme CHECK Team Leader (CTL / SST)
Industrial Control Systems / Operational Technology Experts	*Optional if a department requires Operational Technology ExpertsDepartments will be able to clarify further specific requirements from companies.*

12. Price

12.1 Prices are to be submitted via the attached Pricing Schedule excluding VAT.

12.2 This contract is based on Fixed Price.

12.3 T&S is not applicable for this contract.

13. Staff and customer service

13.1 The supplier shall ensure that its staff have a good understanding of DVLA vision and objectives, knowledge of the CAF, as well as providing excellent customer service to the buyer throughout the duration of the contract.

13.2 Please see below the expected level of experience and expertise of the required suppliers project staff.

13.2.1 The Supplier's staff assigned to the contract shall have an excellent understanding of:

13.2.1.1 The National Cyber Security Centre's Cyber Assessment Framework

13.2.1.2 Cyber audit and risk management, and technical cyber security expertise.

13.2.2 Working with HM Government

13.2.3 Supplier staff engaged in undertaking this work will hold at least SC clearance.

13.2.4 one of the systems involved has a significant mainframe component, therefore experience with mainframe security would be highly advantageous.

14. Security and confidentiality requirements

14.1 The supplier should be familiar with working with HM Government. They should have SC and adhere to DVLA data confidentiality agreements. The supplier should use departmental systems and IT when conducting the assurance review to ensure Driver and Vehicle Licensing Agency information remains on DVLA's network and systems. Driver and Vehicle Licensing Agency will decide on the best way to share information and data, however, DVLA information and data should not sit on the supplier's network or devices.

14.2 Following the completion of the assurance review, the findings of the independent assurance review will only be shared with DVLA, supplier and Government Security Group.

15. Payment and invoicing

15.1 Invoices should be submitted to:

Email: **ssa.invoice@sharedservicesarvato.co.uk**

Postal Address: Shared Services arvato
5 Sandringham Park
Swansea Vale
SA7 0EA

16. Contract management

16.1 Attendance at contract review meetings shall be at the supplier's own expense.

16.2 The following communication stages are required from both parties to ensure contract fulfilment. These stages include the following meetings:

16.2.1 An initiation meeting with relevant parties from both the Buyer and Supplier to commence the project.

16.2.2 The Supplier will attend regular progress update calls at the beginning and end of each week.

17. Location

17.1 The supplier is required to undertake the work remotely however this must be undertaken from locations within the UK.