Driver & Vehicle Licensing Agency

Specification

Provision of a Direct Debit Solution

Operations & Customer Service Directorate (OCSD)

Contract Reference: PS/23/05

Date: 09.01.2024
Version: 1.0

April 2023

1. Introduction **3**

2. Background to the Requirement **5**

3. Procurement Timetable **6**

4. Scope **6**

5. Implementation and Deliverables **9**

6. Specifying Goods and / or Services **11**

7. Social Value Considerations **40**

8. Quality Assurance Requirements **45**

9. Other Requirements **46**

10. Management and Contract Administration **56**

11. Training / Skills / Knowledge Transfer **58**

12. Documentation **59**

13. Arrangement for End of Contract **62**

14. Evaluation Criteria **63**

15. Points of Contact **65**

16. Annexes: **66**

Annex 2 – Welsh Language Scheme Requirements 72
Annex 3 – DD Overview Service Model Diagram 72
Annex 4 – Employee Liability Information TUPE 72
Annex 5 – Procurement Counter Fraud Statement 73

1. Introduction

The Driver and Vehicle Licensing Agency (DVLA), on behalf of the Department for Transport (DfT) invites proposals for the provision of a Direct Debit (DD) solution for the collection of Vehicle Excise Duty (VED). This contract will be subject to the Mid-Tier Terms and Conditions of Contract. This Procurement will be subject to an Invitation to Tender (ITT).

1.1 Definitions

The definitions are as follows:

The Authority	means Driver and Vehicle Licensing Agency (DVLA)
The Supplier	means the party identified as such in the Contract, who is also identified as the Service Provider in connection with the Contract
Commencement Date	1st June 2024
Expiry Date	31st May 2026 (initial contract duration expiry date) 31st May 2027 (This date only becomes applicable should the 1-year optional extension be utilised by The Authority)
Contract Period	means the term of the contract from the Commencement Date until the applicable Expiry Date.
Services	means the various transaction types processed by DVLA.
Contracts Finder	means the Government's publishing portal for public sector procurement opportunities. Contracts Finder allows users to view and search opportunities that are currently open to tender, pipelines of potential procurement activity and awarded contracts.
SME	means an enterprise falling within the category of **micro, small and medium-sized enterprises** defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.
VCSE	means a non-governmental organisation that is value-driven, and which principally reinvests its surpluses to further social, environmental or cultural objectives.

End User	DVLA Customer who uses the Direct Debit payment method to pay Vehicle Excise Duty (or any other applicable Service) prior to this contract commencement, throughout the lifetime of this contract and after its expiry)
Under-represented	can include but is not limited to people with disability, people from working class backgrounds, people from the LGBTQIA+ community, and people from Black, Asian, traveller, mixed heritage or other global majority backgrounds

1.2 Contract Prerequisite

The Supplier must be able to work with The Authority's current IT Infrastructure, enabling a smooth transition of DD Service and ensuring service continuity. E.g. Migration of current Customers Mandate's that are scheduled for automatic renewal.

The Supplier will also support future IT Changes and/or Service Enhancements as they evolve through the Contract Period.

During the Contract Period, there is potential for a new Sponsoring Bank to be appointed by Government after completion of a successful procurement for the Money Transmission Service (MTS) contract. The Supplier must be able to work with The Authority's current Sponsoring Bank Barclays (1 Churchill Place, London, E14 5HP. Companies House Number: 01026167) as well as any different supplier appointed.

To demonstrate The Supplier's capability to address any change required as a result of a change to DVLA's Sponsoring Bank, The Supplier shall develop and provide The Authority with a comprehensive plan to transition The Authority onto the new Sponsoring Bank. This plan must be shared with The Authority prior to the go live date of the MTS Contract. The Supplier shall work in collaboration with the Sponsoring Bank where required to effect transitional/exit arrangements, using commercially reasonable endeavours to deliver the transition, in addition to any applicable End User third party providers such as relevant subcontractor(s) or partner(s) where necessary.

Changes that must be addressed in the plan are including but not limited to;

- Transfer of service user numbers (SUNs)/new SUNs provided from Barclays to new supplier.
- Transfer of existing DD mandates and indemnities. New indemnities after incumbent contract expires.
- The Authority's existing Front Office Counter Services (FOCS) currently provided by the Post Office. **Redacted under FOIA section 43(2).**

2. Background to the Requirement

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

A DD payment option was introduced from 1st October 2014 which enables End Users to currently pay the full annual VED amount in one annual instalment, pay for a 6-month licensing period in one instalment or opt to spread the costs evenly over the term of a 12-month licensing period.

In the future other payment option frequencies must be available at The Authority's request. All options result in an automatic VED renewal, subject to all business requirements being met, unless the End User opts out of the DD scheme.

- Currently, over 1.3 million mandates are created per month, this is split between circa new (40%) and renewed (60%) mandates.
- On average, Direct Debit payments total approximately £225m a month.
- The total value of the contract for the financial years 2018-2023 is in the region of £25 million

Accuracy of the Data

The Authority shall take all reasonable steps to ensure that the Data is accurate and up to date before it is transmitted to The Supplier, but The Authority cannot warrant for the accuracy of the Data provided. The Authority does not accept any liability for any inaccurate information supplied to it by the End User and or any other source beyond its control.

The Authority agrees that The Supplier shall not be liable for any inaccurate information supplied to it by The Authority, the End User or any other source beyond The Supplier's control.

Redacted under FOIA section 43(2)

The Authority seeks to appoint a Supplier to administer and manage the DD payment service via a contract that shall be for an initial contract duration of 2 years commencing on 1st June 2024 with an option to extend for 1 further period of 12 months, to be determined annually at The Authority's sole discretion, to 31st May 2027.

For the purpose of Data handling within this contract, The Authority is the Data Controller and The Supplier is the Data Processor. Both Parties shall act in accordance with the principles of Data Protection legislation within their identified roles.

The Supplier will not be provided with access to the vehicle record for the provision of the Services.

3. Procurement Timetable

The timetable for this Procurement is set out in the ITT document. This timetable may be changed at any time but any changes to the dates will be made in accordance with the Regulations (where applicable).

Potential tenderers will be informed if changes to this timetable are necessary.

Duration of Contract.

The duration of the Contract shall be for 2 years, with the option of a 1 Year extension to 31st May 2027.

Following expiry of the contract, The Supplier shall be allowed a maximum resolution period of up to 1 month from the expiry date, to resolve all payment failures. During this period the requirements and standards detailed within this specification shall still apply as will the Terms and Conditions of the contract.

4. Scope

4.1. General scope of the Service

4.1.1 A DD Creation Service offered via The Authority's Online Electronic Vehicle Licensing Service (EVL) and via The Authority's existing Front Office Counter Services (FOCS) currently provided by the Post Office. The option to add an Agent Telephone Channel is also to be explored.

4.1.1.1 These services are built on Legacy systems, **Redacted under FOIA section 43(2).** There may be a requirement from The Supplier to work together with The Authority during the period of the contract to enable transition from the current systems to any new systems **Redacted under FOIA section 43(2).** The Supplier is to comment on and outline, their ability to adapt to new technology (Cloud Base / API etc).

4.1.2 The creation of the Direct Debit instruction (DDI) will be via the Automated Direct Debit Instruction Service (AUDDIS) within 1 working day.

4.1.3 Creation of payment schedules, sharing with The Authority and End User. For the avoidance of doubt, the Authority shall engage the email provider directly (Amazon SES as at the Start Date) and shall ensure that any contract allows the Supplier to make use of the services.

4.1.4 The Authority shall not store the DDI details on its systems and expects The Supplier to hold End User details. The Authority must be able to view

End User detail and update personal data, via an Authority accessible portal/interface.

4.1.5 Managing monthly DD payment & collection processes, unless otherwise defined by The Authority.

4.1.6 Financial reconciliation to be provided to DVLA on a monthly basis (see section 6.14.10), with annual summary at year end, The Authority's year end is 31 March. (Financial reconciliation and annual summary shall be open to audit, as required by The Authority).

4.1.6.1 Annual Assurance statement to an appropriate standard (minimum of ISAE 3402 Type 2) to give assurance of the sums collected (completeness of income) and provide ISAE 3000 for bank reconciliation of the DVLA Government Banking Service (GBS) bank accounts to support The Authority's annual report and accounts, both audit reports are required by the end of April each year. In addition, The Supplier shall keep a watchful eye on the progress of ISO20022 and if this rolls out to Direct Debits or Direct Credits during the life of the new contract, The Supplier must be compliant before this becomes mandatory for Direct Debits. More information about the ISO20022 standard can be found here: https://www.iso20022.org/

4.1.7 Refunding overpayments via a Direct Credit function including notifying the End User and The Authority of payment failures and failure reasons.

4.1.8 The Data migration of existing DD End Users from the incumbent supplier to the new service, including existing databases (see 4.1.9). The approach for this is to be confirmed i.e. a full switch over of all the service on a given date or a stepped approach over a period of time. This will be discussed with The Supplier.

4.1.8.1 The Supplier will be required to work with the exiting supplier and The Authority to ensure smooth and timely transition of the service.

4.1.9 The Supplier shall provide information to The Authority on Customers who default on payment for a specified number of times. The Supplier should provide the information by bank account or Vehicle Registration Number (VRN) and have systems in place to prevent these customers from setting up further DDIs. The rules for the number of failures will be defined by The Authority and should be configurable. See Section 6.2.10.

4.1.10 The Supplier will support sending out ad-hoc email at The Authority's request (i.e. exceptional circumstances), such ad-hoc requests shall be

handled in accordance with the Variation Procedure. If this requirement is called upon due to an error from The Supplier, the service will be provided free of charge.

4.2 Instructions regarding requirements:

Section 6 of this document stipulates the requirements for this procurement.

Each section describes the **Mandatory Requirements and Optional Requirements.**

For the **Optional Requirements** The Supplier will need to provide indicative costs and specify if they will be able to deliver:

(1) As a change request (CR) cost to be delivered during the agreed contract

The Authority understands that the costs provided for these items will be estimated based on The Suppliers' understanding of the requirement and is subject to change. As such The Supplier is to provide costs in the form of a value range. (e.g. £10K to £20K)

(2) As part of the initial contract delivery cost

The Authority understands that the costing provided for these items will be estimated based on The Suppliers' understanding of the requirement and is subject to change. As such The Supplier is to provide a comparative costing of this estimate. (e.g. £10K to £20K as a CR, £4K to £8K as part of initial contract delivery)

For the **Optional Requirements** The Supplier is asked to comment on:

- The Suppliers ability to deliver such a requirement.
- Whether the requirement is something they offer as Business as Usual (off the shelf) or whether it would need to be delivered as a bespoke piece

4.3 Excluded from the scope:

4.3.1 The printing and dispatch of paper schedules & letters to End Users who do not provide e-mail addresses.

4.3.2. Provision of Call Centre Services for DD Services

4.4 Estimated Volumes

Forecast volumes for Number of End Users re-licensing using the DD process for June 2024 to May 2027 are outlined below. These volumes and channels are for

indicative purposes only and may be subject to change. No minimum or maximum volumes are guaranteed.

	Month	Jun 24 - May 25	Jun 25 - May 26	Jun 26 – May 27
DD EVL	Forecast Volume	6,394,435	6,397,052	6,399,618
DD Post Office	Forecast Volume	130,802	128,187	125,623
DD Renewals	Forecast Volume	10,023,849	10,023,849	10,023,849
TOTAL DDs	Forecast Volume	**16,549,086**	**16,549,088**	**16,549,089**

- It is to be noted that through the lifecycle of a mandate a volume of activities can occur increasing the “transactions” required against each mandate such as receipt of cancellations etc.
- It is to be noted that through the Lifecycle of the mandate each renewal can result in increased activity such as re-presents of failed payments etc.
- The Authority will review and provide The Supplier with updated forecasts on a quarterly basis to ensure The Supplier has sufficient capacity to deal with volumes. The Supplier shall ensure they have the resources, assets and technology infrastructure to meet the minimum forecast volumes for the Service.
- The Supplier shall have the ability to **scale the Service** to meet demand and shall provide an indication in its response of how quickly the Service can be expanded to meet any increase in demand, or addition of other transactions to its DD solution.
- DD volumes will increase with the introduction of VED for Electric Vehicles in 2025. Updated forecast will be provided when available.

5. Implementation and Deliverables

The Commencement Date of the contract is 1st June 2024. Following Contract award, The Authority requires The Supplier to provide a transition plan for existing customer DD mandates. All DD Mandate transition activities must be identified, captured, prepared, tested and ready for deployment at least 2 months prior to the commencement date of contract (i.e. 1st April 2024), to provide confidence and ensure continuity of Service of DD Instructions.

The Supplier shall develop a plan to transition The Authority onto the new DD Contract. This plan must be shared with The Authority within 1 month following

contract award. The Supplier shall work in collaboration with the incumbent Supplier(s) to effect transitional/exit arrangements, using commercially reasonable endeavours to deliver the transition, in addition to any applicable End User third party providers such as relevant subcontractor(s) or partner(s) where necessary.

The Supplier shall manage the implementation of the Deliverables into The Authority's organisation, within a timescale agreed between The Authority and The Supplier in the new DD Contract.

The Supplier shall work with The Authority to agree an implementation plan to transition any existing DD mandates and related payment acceptance information identified within the scope of the new DD Contract. This must be completed 2 months prior to the contract commencement date.

The Supplier shall provide an implementation plan which sets out how The Authority's Deliverables will be implemented. The implementation plan shall include, as a minimum standard, the following elements:

- project plan including timescales.
- project management methodology as agreed between the parties, including a process for reporting progress against agreed plans.
- an implementation team structure, including a named implementation manager and named technical experts.
- a detailed plan of how data will be securely transmitted and stored throughout the Contract Period.
- a testing and acceptance plan, which must include:
    - undertaking user training
    - issuing user guides; and
    - carrying out test process dry runs.

5.1 Key Milestones

The Supplier shall note the following key milestones, in accordance with agile methodology, that The Authority shall measure the quality of delivery against:

Milestone	Description	Timeframe
1	Service Discovery - Initial stage to define and agree the detailed approach for working with The Authority to design, build, test and implement an end-to-end solution	Within week 1 of Contract Award
2	Service inception - To develop a detailed solution and implementation plan to achieve the required go-live date	Within week 2-4 of Contract Award
3	Delivery of Alpha Release - if deemed applicable as a result of the Discovery and Inception stage	Prior to contract commencement.

	To deliver a working proof of concept (the scope and nature of which will be defined within the Discovery and Inception stages)	
4	Delivery of Beta Release(s), following Alpha and deliver working software into a live environment	Prior to contract commencement.
5	Service Go live.	Prior to contract commencement.

6. Specifying Goods and / or Services

6.1 General Requirements:

6.1.1	The Supplier shall provide a brief background on its organisation, stating whether it is a Bankers Automated Clearing Service (BACS) approved bureau and / or BACS approved software provider (and AUDDIS compliant). The Supplier must provide evidence or proof of accreditation or Standards. E.g. a Certificate	Mandatory
6.1.1.2	The Supplier shall confirm and provide evidence that they are fully compliant with the current Direct Debit and Bacs Direct Credit Scheme Rules.	Mandatory
6.1.1.3	The Supplier shall remain compliant with Direct Debit and Bacs Direct Credit Scheme Rules throughout the Contract Period (Including extensions)	Mandatory
6.1.2	The Supplier shall state which software solution is being proposed and state whether the entire solution or just the BACS submission mechanism is BACS accredited.	Mandatory
6.1.3	The Supplier is required to apply the rules of the DD Scheme and operate within the set procedures as defined within the Direct Debit Service User Guide & Rules. https://www.bacs.co.uk/sugr/pages/sugrdd.aspx	Mandatory
6.1.4	The Supplier shall ensure any delivery of the Services provided by third parties is in accordance with the Specification and shall manage the relationship with the third parties to ensure the services are delivered in accordance with the Requirements. Before allowing any third party (who would act as a Sub-processor) to process any Personal Data related to this Agreement, the Processor must: (a) notify the Controller in writing of the intended Sub-processor and processing. (b) obtain the written consent of the Controller. (c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause such that they apply to the Sub-processor; and provide the Controller with such information	Mandatory

regarding the Sub-processor as the Controller may reasonably require.

(d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require

6.1.5	The Supplier will ensure that all practices abide by the requirements of all relevant data protection legislation: (a) the UK GDPR as amended from time to time (b) the DPA 2018 to the extent that it relates to processing of personal data and privacy. (c) all applicable Law about the processing of personal data and privacy. (d) the EU GDPR where applicable to the processing.	Mandatory
6.1.6	The Supplier shall 'stand up' a Project team, to deliver this initiative working collaboratively with The Authority. The Supplier and The Authority's joint Project Team will work together ensure a smooth transition and to implement the Service within the timescales defined (to include a period of on-boarding) to ensure a June 2024 exit of incumbent Supplier.	Mandatory
6.1.6.1	The Supplier is required to outline the predicted required timescale from Contract Award to Service Go live based on their understanding of the requirements. This will help The Authority understand the transitional timeline from the current to the new contract for this service.	Mandatory
6.1.7	The Supplier shall manage the interactions, payment and notification files between its system and BACS. The Supplier shall provide all required data feeds. E.g. (including but not limited to) notification of failed, cancelled DDIs or Indemnity Claims (with the lower-level reasons for in each case). The Authority will use the data to update vehicle records and initiate any necessary resultant enforcement activity.	Mandatory
6.1.7.1	The format and frequency of all notifications and data received/sent will be agreed by The Authority in conjunction with The Supplier.	Mandatory
6.1.7.2	The Supplier is to provide a brief description as to how they will be able to provide all agreed data feeds.	Mandatory
6.1.8	The integration points between The Authority and any other Supplier must conform to open (or industry) standards. https://www.gov.uk/government/publications/open-standards-principles	Mandatory
6.1.9	The Supplier shall provide capacity to increase transaction volumes and/or add additional Services. Subject to agreement, The Authority may wish to add additional DD Services in future. This may include the onboarding and integration of newly designed or existing Digital Services.	Mandatory
6.1.10	The Supplier shall support the transition of elements of an overall DD service from The Supplier to The Authority, whilst minimising costs and	Optional

	penalties if requested. e.g. the online capture screens, email notification(s) functionality. The Authority may use its own Notifications Utility (**Redacted under FOIA section 43(2)**) for End User emails. The Supplier must outline how they will support The Authority to deliver this solution with no (or minimal) cost.	
6.1.10.1	The Supplier shall explain how they propose to support The Authority through potential activities.	Optional
6.1.10.2	The provision of functionality to allow the End User to access their payment details to view payment schedules and change (update name, addresses and bank account details) either through an End User self-service portal or through APIs that The Authority could use to build such a portal.	Optional
6.1.11	There shall be no changes to the Service(s) delivered without the prior written agreement of The Authority. This includes Business as Usual, Scheduled/Planned and Emergency Changes. A Change Delivery Roadmap must be shared with The Authority and agreed post contract award.	Mandatory
6.1.12	The Supplier shall be expected to continually improve the way in which the service(s) is to be delivered throughout the Contract. E.g. industry best practice, technological advances, Service Improvements (potentially in line with legislative changes). These will be delivered in accordance with the Variation Procedure.	Mandatory
6.1.13	The direct debit system(s) must be uploaded with BACS EISCD (sort code updates) updates on a weekly basis within 5 working days of receipt.	Mandatory
6.1.14	The Supplier shall present new ways of working to The Authority as part of continuous service improvement throughout the contract term.	Mandatory
6.1.15	During the Term of the Contract (including any Extension Periods) The Authority and The Supplier shall work together if required by The Authority on potential future opportunities to improve the Services and drive efficiencies.	Mandatory
6.1.16	The Authority is engaging in significant portfolio of change which may result in changes to its requirements and strategy during the term of the contract. The Supplier is asked to explain how it will support The Authority through this heavy change program. (i.e. SME support, Change Pipeline planning, delivery/development resource availability, reduced daily rates etc.)	Mandatory
6.1.17	The Supplier shall confirm that in the event the MTS results in a change of banking provider, The Supplier will provide a comprehensive plan to transition The Authority onto a new Sponsoring Bank and will actively work with The Authority	Mandatory

6.2 Direct Debit Creation Service

6.2.1	The Supplier shall provide a paperless DD creation Service, with Web Screens to capture Customer data that must comply to the Government Digital Service (GDS) Service Standards. The Service must be consumable from the DVLA web and Post Office TM Counter channel. The Authority may wish to explore an Agent Telephone Channel also. The provision must include input and output data exchange for the whole process which complies with the relevant interface specification. (Also see 6.2.13 Optional channel below)	Mandatory
6.2.2	The Service shall be hosted within a secure and controlled application environment.	Mandatory
6.2.3	The Service shall enable End Users to pay the full Vehicle Excise Duty (VED) amount in one annual instalment, pay for a 6-month licensing period in one instalment or opt to spread the costs over the term of a 12-month licensing period. The three options will result in an automatic VED renewal, subject to all business requirements being met, unless the End User opts out of the DD scheme.	Mandatory
6.2.4	A 21-digit unique Customer Reference Number (CRN), generated by The Authority, and the data provided by the End User including, but not limited to, name, address, bank details and email address shall be captured by a defined/agreed 'Service Solution Technology' and processed together with the total VED amount payable and payment option to the DD creation Service. The DD creation Service will accept and store, in accordance with The Authority's security requirements all the details provided. The unique CRN will be used by The Authority to link a vehicle licence record with the DDI.	Mandatory
6.2.5	The Supplier will ensure that the information captured at the point of creation is correct. Including but not limited to, e.g. email addresses are entered in the valid field only, formatting is correct.	Mandatory
6.2.6	If the data provided by the End User is successfully processed the DD Creation Service will provide The Authority's system with a positive response which will be passed to the End User in real-time either online, Agent channel or at the Post Office TM Counter.	Mandatory
6.2.7	If the data provided by the End User is successfully processed the DD creation Service will prevent the End User from setting up duplicate mandates on that specific vehicle for a period of time, **Redacted under FOIA section 43(2)**, however this shall be configurable at The Authority's request.	Mandatory
6.2.8	An email notification confirming the set-up, payment schedule and the DD guarantee shall be provided/sent to The End User within 24 hours from the time of transaction. (The Authority may use its own Notifications Utility for this function.)	Mandatory

	Where an email address is not available or an invalid email address is provided, The Supplier shall provide The Authority with a Notification (e.g. file with payment schedule details) capturing all the schedule details for printing at DVLA within 24 Hours.	
6.2.9	If the data provided by the End User is not successfully processed the DD creation Service shall provide The Authority system with a 'negative response' including failure reason which will be passed to the End User in real-time either online, Agent channel or at the Post Office TM Counter. The End User shall then be presented with the option to retry or pay by alternative means within the transaction.	Mandatory
6.2.10	The Supplier will support The Authority in designing/delivering functionality to Sanction/Block and prevent certain End Users from applying for a new DD. This will be based on a set criteria and eligibility rules, defined by The Authority. Solution must be completed prior to date of contract commencement.	Mandatory
6.2.11	The Supplier will need to accept the migration of the existing register of Sanctions/Blocked End Users from the incumbent Supplier's system.	Mandatory
6.2.12	**Redacted under FOIA section 43(2)**	**Redacted under FOIA section 43(2)**
6.2.12.1	**Redacted under FOIA section 43(2)**	**Redacted under FOIA section 43(2)**
6.2.13	**Redacted under FOIA section 43(2)**	**Redacted under FOIA section 43(2)**
6.2.14	**Redacted under FOIA section 43(2)**	**Redacted under FOIA section 43(2)**

6.3 Direct Debit Renewal Function

6.3.1	Before commencement of a new licensing period, all business requirements must be met to enable the automatic renewal of a new licensing period. The Supplier must act upon the information and criteria provided by The Authority.	Mandatory
6.3.2	Following successful checks, The Authority shall notify The Supplier that they may create the renewed mandate. The Authority shall supply the applicable VED rate and payment period to The Supplier.	Mandatory
6.3.3	At point of DD renewal (licence period expiry) The Supplier shall not create a renewed mandate and take any further payment from the End User until they have received the renewal confirmation Notification from The Authority which includes applicable VED rate and payment period.	Mandatory

6.3.3.1	Renewal Notifications can be sent up to five days after the expiry of the licensing period however in most instances shall be provided several weeks in advance and follow an agreed schedule of which both The Authority and Supplier have agreed.	Mandatory
6.3.4	If authorisation to proceed is provided too late to collect payment on the 1st working day of the month, the 1st payment of the next licensing cycle shall be taken as soon as the BACS approved period has lapsed. The 2nd payment will be taken on the 1st working day of the second month.	Mandatory
6.3.5	Following authorisation, The Supplier shall notify The Authority and/or End User within 24 Hours. A payment schedule will be issued via e-mail to the End User where an email address is available. (The Authority may use its own Notifications Utility for this function.) If no email address is provided, The Supplier shall provide The Authority with a Notification that capturing the schedule details for printing at DVLA within 24 Hours.	Mandatory
6.3.6	Where a DD mandate settles or does not 'auto renew' and an email address is available for the End User, an email must be sent to the mandate holder to advise/prompt action. i.e. where a DD does not renew and is not cancelled. (The Authority may use its own Notifications Utility for this function.)	Mandatory

6.4 Duplicate Payment Schedules

6.4.1	The Supplier must provide The Authority the functionality to issue a duplicate payment schedule to the End User via email if an email has been provided. (The Authority may use its own Notifications Utility for this function.)	Mandatory
6.4.2	The Supplier must provide The Authority the functionality to issue a duplicate payment schedule to the End User via paper if an email has not been provided (make a print version available). The paper schedule will be sent by The Authority, on receipt of a Notification from The Supplier.	Mandatory

6.5 Content of Correspondence

6.5.1	All correspondence shall be issued in line with BACS requirements and Standards. http://www.bacs.co.uk/bacs/sugr/pages/serviceusersguide.aspx	Mandatory
6.5.2	All correspondence will be issued by The Authority, unless otherwise stated or requested. If (subject to request by The Authority) issued by The Supplier, correspondence shall appear as	Mandatory

	though it has originated from The Authority even though it may be generated from The Supplier's system.	
6.5.3	The content and style of the communication shall be agreed with The Authority prior to issue.	Mandatory
6.5.4	The Supplier shall ensure that all communications shall include the unique CRN and VRM associated with the vehicle.	Mandatory
6.5.5	Where a mandate schedule email fails to be sent successfully to the End User, The Supplier shall provide The Authority with the End User details (Notification) so that The Authority can print paper copies and send by post. This process could be applied to any email issue at The Authority's request.	Mandatory
6.5.6	**Redacted under FOIA section 43(2).**	**Redacted under FOIA section 43(2)**
6.5.6.1	**Redacted under FOIA section 43(2).**	**Redacted under FOIA section 43(2)**

6.6 Unsuccessful instruction set-up

6.6.1	If a DDI is rejected at set-up by the paying bank, The Supplier must inform the End User via an immediate onscreen notification. Where The Supplier has an email address for the End User, an email must be sent advising of the rejection. (The Authority may use its own Notifications Utility for this function.) Also, a record should be sent in a bulk cancellation file (or alternative solution) from The Supplier to The Authority so their records can be updated.	Mandatory

6.7 Instruction amendments and cancellations

6.7.1	The Supplier must provide The Authority the functionality to amend mandates to update name, postal address, email address and/or bank details on a DDI, retaining the same licensing period and payment dates where applicable. The same level of verification and checking as at set-up must apply. (Direct Debit Creation Service Section 6.2)	Mandatory
6.7.2	The Supplier shall action any mandate change notifications received via the BACS automated notification process within 1 working day.	Mandatory

6.7.3	Cancellation notifications may be received by The Supplier from the End User's bank, or from The Authority. This can be submitted either in Bulk or through individual cancellations initiated by The Authority. Cancellations received from the End User, or their bank shall be notified to The Authority. The Authority will notify The Supplier of a cancellation in various. circumstances, such as on receipt of a notification from the End User of the vehicle having been exported, scrapped or transferred. Notification to cancel an instruction must be actioned by The Supplier within 1 working day where a payment has not already been requested.	Mandatory
6.7.3.1	If an email address is provided, The Supplier shall notify The End User of the cancellation of the mandate within 24 Hours (The Authority may use its own Notifications Utility for this function.) If no email address is provided, The Supplier shall provide The Authority with a file (or Notification) for printing at DVLA within 1 working day (The Authority will decide how this Notification is actioned).	Mandatory
6.7.4	In the event of a late notification of cancellation from The Authority and after the money has been successfully received, (e.g. a payment has been taken at the start of the month but the keeper has advised of vehicle disposal prior to the collection or the request for collection has already been made), The Supplier shall be able to arrange for a refund via a Direct Credit Service as advised by The Authority directly into the End User's bank for the amount the End User was not required to pay within 5 working days.	Mandatory
6.7.5	The Supplier shall provide The Authority with the ability to process manual cancellations and requests via an Authority accessible portal/interface/API. For further details please refer to Section 6.12 (End User Enquiries).	Mandatory
6.7.6	The Supplier shall provide functionality to set the mandate account status to "Pending cancellation" to allow a period of time for in-flight payments to process or be returned as unpaid. This is to prevent the system from paying incorrect refund amounts to the mandate holder.	Mandatory
6.7.7	The Authority will provide The Supplier with a list (e.g. file) advising of VRN changes. The Supplier will update the customer mandate to reflect said change within 24 Hours. The Supplier will advise The Authority if/when this cannot occur.	Mandatory
6.7.8	If an email address is provided, The Supplier shall notify The End User of a pending customer reimbursement within 24 hours, providing a timescale for receipt of the reimbursement. (The Authority may use its own Notifications Utility for this function.)	Optional

6.8 Collection Process

6.8.1	The Supplier shall ensure that the End Users are able to set-up a DD from the 1st of the month prior to their VED being due, to the last day of the month in which the VED is due e.g. VED due 1st November, a DD can be set-up from 1st October to 30th November. End Users cannot backdate VED, if it is over 1 month since it was due, i.e. if the VED due 1st November, a DD cannot be set up by the End User on 1st December. The Authority business rules prevent this from occurring.	Mandatory
6.8.1.1	The Supplier shall be able to configure their business rules should The Authority's business rule change. This shall be subject to formal change request.	Mandatory
6.8.2	Collections shall be taken from the End User's bank account on the 1st working day of the month that the payment is due providing appropriate payment schedules have been issued in line with the BACS approved period.	Mandatory
6.8.3	If the VED is purchased during the month of commencement the first payment shall be taken as soon as the instruction is active, Subsequent payments shall be taken on the 1st working day of the month. This must be communicated to the End User as part of the payment schedule.	Mandatory
6.8.4	If the VED is purchased so late in the month of commencement that the DD is not set up until after the 1st of the following month, two months payments shall be taken as soon as the instruction is active. Subsequent payments shall be taken on the 1st working day of the month. This shall be communicated to the End User as part of the payment schedule.	Mandatory
6.8.5	Collections/payments are made via daily BACS files per bank account into a DVLA GBS (Government Banking Service) bank account to be managed and reconciled by The Supplier. The Supplier shall state how many daily files would be required to accommodate The Authority's volumes. The Authority shall automate a monthly sweep of funds at a time to be determined by The Authority and GBS. (The Authority is open to considering alternative Solutions or methods of secure Data Transfer and integration.)	Mandatory
6.8.6	The Supplier shall notify The Authority daily of any unreconciled items for further investigations within two calendar days of date of account.	Mandatory

6.9 Failed Collections

6.9.1	For collections which fail due to insufficient funds, The Supplier shall re- present 4 working days after the 1st collection attempt (configurable at The Authority's request). If this is a non-banking	Mandatory

	day, representation should take place on the next available working banking day.	
6.9.1.1	The Supplier will only attempt to collect the amount set out in the payment schedule (no additional charges will apply to The Authority for any failed collections).	Mandatory
6.9.2	Where The Supplier has an email address for the End User, The Supplier shall notify The End User advising of the failed collection from customer and the upcoming second attempt within 1 working day. (The Authority may use its own Notifications Utility for this function.)	Mandatory
6.9.3	For collections that fail on re-presentation The Supplier shall cancel the DDI. [see related requirement 6.7.3.1] For all failures, including where the 2nd collection fails, an electronic 'notification' (e.g. File) shall be provided to The Authority detailing the failures and quoting all the applicable information. This will include but is not limited to, appropriate failure code and the unique CRN in accordance with the interface specification. Where The Supplier has an email address for the End User, The Supplier shall notify The End User of the cancellation within 1 working day of receipt from the bank. (The Authority may use its own Notifications Utility for this function.)	Mandatory
6.9.4	The Supplier is to confirm that a Report of all Failed Payments will be provided in a simple 'format' to enable MI manipulation (filtering, sorting) for service reporting purposes.	Optional
6.9.5	The Supplier will automatically cancel mandates on receipt of an Indemnity Claim that is in relation to a live mandate. The Supplier must Notify the End User within 24 hours. (The Authority may use its own Notifications Utility for this function.)	Optional

6.10 Indemnity Claims

6.10.1	The Supplier must process indemnity claims made by the End User in line with the terms of the Direct Debit guarantee. Details of all indemnity claims, along with any evidence provided by the claimant's bank, shall be uploaded to the End Users account which is held by The Supplier within 48 hours.	Mandatory
6.10.2	The Authority shall use this data to update their vehicle records and initiate any resultant enforcement activity. The value of funds will be automatically taken from the DVLA GBS bank account managed by The Supplier and included on the reconciliation statement.	Mandatory
6.10.2.1	**Redacted under FOIA section 43(2).**	**Redacted under FOIA section 43(2)**

6.10.3	**Redacted under FOIA section 43(2).**	**Redacted under FOIA section 43(2)**
6.10.4	**Redacted under FOIA section 43(2).**	**Redacted under FOIA section 43(2)**

6.11 Complaints

6.11.1	The Supplier shall provide written contributions to complaints received by The Authority within 7 working days of receipt of a contribution request from The Authority.	Mandatory
6.11.2	The Supplier shall provide contributions to official correspondence (e.g. Ministerial or MP letters; Freedom of Information or Data Subject Rights requests; Fraud Investigations) within short timeframes, to be agreed at the point of request although typically within no more than 5 working days of a written request from The Authority.	Mandatory

6.12 End User Enquiries

6.12.1	The Supplier shall provide an interface (i.e. enquiry and amendment facility) via an Authority Accessible portal, on a two-tier access model, to the details held within the DD system to enable The Authority or its agents to deal with Customer (End User) enquiries and change requirements. The 'Portal' may be hosted by The Supplier or The Authority and is dependent on solution proposed and jointly agreed. E.g. Functionality provided with Exposed APIs by Supplier.	Mandatory
6.12.1.1	Training material and User guides are to be provided to The Authority by The Supplier (if relevant).	Mandatory
6.12.1.2	The Supplier is to confirm if there are limits to the volume of users which can be given access to the interface, and what the limit is. **Redacted under FOIA section 43(2).**	Mandatory
6.12.2	The Supplier shall provide a help desk function as specified to deal with DD related casework queries from The Authority.	Mandatory
6.12.3	The Supplier is to work closely with The Authority to develop or adapt the interface which is suitable for the purpose of The Authority's contact centre and operational business areas (dependant on solution proposed/agreed). Any adaptations shall be managed in accordance with the Variation Procedure.	Mandatory

6.12.4	Configurable “time out” settings (ref 12.1) which can be changed by The Authority following a change request.	Mandatory
6.12.5	The Supplier shall work with The Authority to define/agree the content and language used in the mandate diary/system information to ensure ease of use.	Mandatory
6.12.6	The Supplier shall ensure that each cancellation reason displayed has its own individual code attached, instead of a general cancellation code.	Mandatory
6.12.7	All activities relating to access of the interface and specific DDI record will be trackable and can be audited when required.	Mandatory
6.12.8	**Redacted under FOIA section 43(2).**	**Redacted under FOIA section 43(2)**
6.12.9	The Supplier shall provide the ability to view / access multiple mandates related to a specific Vehicle Registration Number.	Mandatory
6.12.10	The Supplier shall provide a mandate search facility using varied search criteria in order to be able to identify mandates with or without mandate ID or Vehicle Registration Number.	Mandatory
6.12.11	The enquiry functionality shall have a search facility to the evader (blocked user) database, with access rights managed by The Authority.	Mandatory
6.12.11.1	The Enquiry functionality will ensure that Information returned from evader search facility confirms reasons for addition to the database. A descriptive field is available against each reason type where The Authority can dictate the information returned to the Agent. i.e. key information to be provided to end-user at the point of contact.	Mandatory
6.12.12	The Supplier shall provide a facility to reinstate mandates which have been cancelled in error (by The End User) within the limits of business rules set by The Authority.	Optional
6.12.13	**Redacted under FOIA section 43(2).**	**Redacted under FOIA section 43(2)**
6.12.14	The Supplier shall provide a trainer for face to face or remote training of The Authority’s agents, if required by The Authority.	Mandatory

6.13 Reporting

6.13.1	The Supplier shall provide Management Information (MI) in a report or data set format to The Authority on a daily, weekly, monthly or yearly	Mandatory

basis as appropriate, in an electronic format. Full MI Requirements shall be agreed by The Authority prior to contract commencement.

6.13.2	The MI reports or data sets shall provide underlying details of the total number and value of mandates to enable formal confirmation of the completeness of income in respect of VED to allow agreement of VED income to mandate reference to facilitate a reconciliation process on a quarterly basis.	Mandatory
6.13.2.1	Reports must include:	
	• The funds successfully collected (breakdown, e.g. one-off annual payment, one off 6-month payment, date of liability etc., to be determined by The Authority).	Mandatory
	• Failed Collections (1st attempt) categorised by reason code plus additional breakdown as determined by The Authority.	Mandatory
	• Failed Collections (re-presented) categorised by reason code plus additional breakdown as determined by The Authority.	Mandatory
	• Reimbursements made	Mandatory
	• **Redacted under FOIA section 43(2)**.	**Redacted under FOIA section 43(2)**
	• **Redacted under FOIA section 43(2).**	**Redacted under FOIA section 43(2)**
6.13.2.2	The Supplier shall notify The Authority daily of all reimbursements (Direct Credits) made to the End-Users, successful and unsuccessful. Format of the MI to be agreed between Authority and Supplier.	Mandatory
6.13.2.3	Direct Credit Report split by Licence start date, channel and Direct Debit type. Direct Credit Report category breakdown format to be agreed between Authority and Supplier.	Mandatory
6.13.2.4	Monthly Reconciliation report file detailing the Total funds collected (gross); total value of failures; total net value collected, total reimbursements and total indemnity claims. Provided in an electronic format, along with a signed PDF. All formats to be agreed between Authority and Supplier.	Mandatory
6.13.2.5	The Supplier shall provide MI on Total Power Consumptions KWhr and energy mix in relation to data hosting.	Mandatory
6.13.3	The Supplier shall provide to The Authority a summary of the monthly total number of End Users for who DD mandates could not be successfully set- up including the reason for the failure	Mandatory
6.13.4	The Supplier shall provide to The Authority a summary of the monthly total number of End Users for who DD mandates have been cancelled including the reason for the cancellation.	Mandatory
6.13.5	The Supplier shall provide, within 10 working days after the Year End (31st March), a report detailing the value due in respect of VED monthly instalments to be settled in the next financial year.	Mandatory

6.14 Financial Reconciliation

6.14.1	The Supplier shall be responsible for daily reconciliation of the DVLA GBS bank accounts and shall pass to the DVLA reconciliation team.	Mandatory
6.14.1.1	The Supplier shall state how this shall be managed.	Mandatory
6.14.2	The Supplier shall be responsible for notifying The Authority within 48 hours where reconciliation has failed.	Mandatory
6.14.3	The Supplier shall provide The Authority's Finance Operations with a report which will include all payments and receipts which have not been presented via The Authority's SUN as part of a Direct Debit or Direct Credit submission.	Mandatory
6.14.4	The Supplier is responsible for providing a list to The Authority of DDI's where a credit/reimbursement is paid in error to the End User.	Mandatory
6.14.5	The Supplier will support The Authority in the reclamation of funds if a credit/refund is paid in error.	Mandatory
6.14.5.1	If VED Revenue is lost because of Supplier action and it is not recoupable, The Supplier shall compensate The Authority.	Mandatory
6.14.6	The Supplier must be responsive to any changes to data fields from BACS or The Authority and be able to maintain the continuity of data feeds when changes arise.	Mandatory
6.14.7	The Supplier shall maintain accurate and auditable records and:	Mandatory
6.14.7.1	shall provide an annual Assurance statement to an appropriate standard (minimum of ISAE 3402 Type 2) to give assurance of the sums collected (completeness of income) and	Mandatory
6.14.7.2	shall provide ISAE 3000 for bank reconciliation of the DVLA GBS bank accounts to support The Authority's annual report and accounts, both audit reports are required by the end of April each year."	Mandatory
6.14.8	Within 10 working days of month end, The Supplier shall provide data that can be imported (e.g. into Excel, CSV) to The Authority detailing the total value of funds collected, net of failures reported to The Authority, during the previous month, split between one-off payments, alternative payments, monthly payments, any refund payments made, the outstanding debt figure and any indemnity claims settled under the DD guarantee. The report should also be provided as a signed PDF to confirm that the reconciliation is complete and accurate.	Mandatory
6.14.9	Within 10 working days of month end, The Supplier shall provide management information (MI) which analyses each month's Direct Debit (DD) receipts between monthly instalments and 6- & 12-month one-off payments, in order to support the reconciliation of receipts from The Supplier to the VSS records.	Mandatory

6.14.10	Financial reconciliation reports to be provided to The Authority on a monthly basis, detailing automated and manual reconciliation.	Mandatory
6.14.10.1	Any outstanding items must be cleared before the following months report.	Mandatory
6.14.10.2	Any outstanding items value must be at zero before the month end.	Mandatory
6.14.10.3	Manually reconciled items must be shared with The Authority once identified with specific reasons and Customer records and mandates to be updated.	Mandatory
6.14.10.4	The Supplier must ensure the accuracy of reconciliation activities and is responsible for providing prompt updates and reports.	Mandatory
6.14.11	The Supplier shall provide a Service Desk to resolve queries raised by The Authority. The Supplier shall have the ability to drill down into the financial details, Reconciliation and resolve queries via the Service Desk.	Mandatory

6.15 Interest on late receipt of Direct Debit funds

6.15.1	Any interruption to the transmission of a BACS file that results in a delay of DD funds being collected into DVLA's Bank Account which is a direct result of a service performance failure by The Supplier will incur a late payment interest penalty (for the purpose of clarity, the definition of a delay is when funds are not collected on the due date). Interest will be payable at a rate of Bank of England Base Rate plus 2% and will be charged on a daily basis from the day on which the money was due and owing up to the actual date of receipt.	Mandatory

6.16 Service and Support Requirements

6.16.1 Service performance

6.16.1.1	The service must be available 24/7/52 in the live environment with a minimum of 99.5% availability per month for all users. The Authority seeks to procure a service that consistently exceeds this, and The Supplier must provide detail of their actual expected availability	Mandatory
6.16.1.2	The service must be able to handle, as a minimum, DVLA's peak business volumes (15 Transactions Per Second (TPS) and average load of 1.5 TPS)	Mandatory
6.16.1.3	Response time per transaction must not exceed 1 second for 99% of transactions	Mandatory
6.16.1.4	The test environment must be available Monday to Friday 06:00 to 18:00 with a minimum of 98% availability per month for all users. The Authority seeks to procure a service that consistently exceeds this, and The Supplier must provide detail of their actual expected availability.	Mandatory
6.16.1.5	The internal Client self-service portal must be available (6am - 8pm 7 days a week) with a minimum of 99% availability per month for all users. The Authority seeks to procure a service that consistently exceeds this, and The Supplier must provide detail of their actual expected availability	Mandatory

6.16.1.6	BACS submissions must be 100% accurate and 99% must be within specified timings (measured monthly)	Mandatory
6.16.1.7	Batch files must be 100% accurate and 99% must be within specified timings (measured monthly)	Mandatory
6.16.1.8	Creation of mandates must be 100% accurate and 99% within specified timings (measured monthly)	Mandatory
6.16.1.9	Collection of mandates must be 100% accurate and 99% within specified timings (measured monthly)	Mandatory

6.16.2 Service support

6.16.2.1	The service must be supported 24/7/365 for, as a minimum Priority 1 and 2 incidents.	Mandatory
6.16.2.2	The Supplier must provide a dedicated business and technical helpdesk 24/7/365 relevant to the Services, accessible by phone, SMS and email and online portal, to include but not necessarily limited to: · Incidents · Problems · Alerts · Queries · Payer queries · Software · Hardware · Complaints	Mandatory
6.16.2.3	The Supplier must define how they prioritise calls and incidents in relation to this service. For example: **PRIORITY: 1** TITLE: Critical DEFINITION: Severe Business Disruption - Service not available. Critical system component failed or severe impairment of on-line systems or batch work including BACS files **PRIORITY: 2** TITLE: Major DEFINITION: Major Business Disruption - Service degraded. Software experiencing significant reduction in system performance, or more than a single user affected by the same incident at the same time. Shall also include the failure of mandate creations or collections, where 10 or more customers are affected by the same issue at the same time. Test environment not available or severely degraded **PRIORITY: 3** TITLE: Medium DEFINITION: Minor Business Disruption. Single incident with no available agreed work-around, or failure in batch processing. Reduction in performance of test environment **PRIORITY: 4** TITLE: Low	Mandatory

DEFINITION: Minor Disruption - Single User incident, but with no direct impact on business, such as a request for information.

PRIORITY: 5
TITLE: Request for Information
DEFINITION: Request for Information, Bug Reporting, FAQs, documentation clarification, and technical guidance for the Software

6.16.2.4 The Supplier must specify their response times for initial response, updates, and resolution. For example: — Mandatory

	Priority 1	Priority 2	Priority 3	Priority 4
Support receipt	5 minutes	5 minutes	1 hour	1 hour
Initial Response	30 mins	1 hour	4 hours	1 Working Day
Update interval	1 hour	2 hours	12 hours	Weekly
Resolution	2 hours	4 hours	1 week	2 weeks

6.16.2.5 The time for the “Support Receipt” in the table above is measured from when The Supplier has been provided with the available relevant information, for the relevant incident report. Initial Reponses shall contain: — Mandatory
a) confirmation of Priority;
b) incident reference number.

6.16.2.6 The time for the “Initial Response” in the table above is measured from when Supplier has been provided with the available relevant information, for the relevant incident report. Initial Reponses shall contain: — Mandatory
a) confirmation of Priority;
b) resolution or Workaround advice, if a Known Issue and such resolution or Workaround readily available to the relevant member of Supplier personnel; and
c) problem reference if applicable;

6.16.2.7 Expected contents of subsequent “Updates” — Mandatory
a) current status;
b) work completed so far;
c) current Investigation direction;
d) restoration estimate ETA; and
e) resolution or Workaround advice.

6.16.2.8 The Supplier must provide detail of their service monitoring provision — Mandatory

6.16.2.9 A Help/Service desk or equivalent must be available 24x7 365 days a year for call logging for, as a minimum, P1 and P2 incidents — Mandatory

6.16.2.10 Where The Supplier detects unusual patterns of activity that might indicate malicious activities, for example a denial-of-service attack or distributed denial of service attack The Supplier shall inform The Authority’s designated security contact immediately by alerting via email and SMS. — Mandatory

6.16.2.11 The Supplier should provide The Authority with the functionality to monitor Supplier’s availability, transaction completion rates and Transaction timings. — Optional

6.16.2.12	Logs in relation to support calls will be maintained by Supplier. Each support call will be recorded by Supplier and will comprise: a) unique reference number of the case; b) the date and time of the call; c) name and contact details of the Incident Reporter reporting the call; d) description of the request or incident being received; e) perceived impact of any incident for users; f) priority of the incident based on the perceived impact; g) reference to any open Problems or Known Errors if known at the time of reporting; h) advice provided to the Incident Reporter including any workaround steps; i) actions taken; j) date and time of resolution; and k) method of resolution.	Mandatory

6.16.3 Incident Management

6.16.3.1	The Supplier must have a defined and detailed incident management process including communication plans, prioritisation levels, response and resolution targets and root cause analysis. Evidence must be provided.	Mandatory
6.16.3.2	The Supplier will provide Error Corrections and correct any other failure, malfunction, defect or non-conformity in the production environment Solution in accordance with the incident management process	Mandatory
6.16.3.3	The Supplier will assist The Authority in identifying, verifying and resolving incidents and defects in the Solution and Software (whether as part of the Solution or as separately licensed Program Product/s).	Mandatory
6.16.3.4	The Supplier must have a defined escalation process.	Mandatory
6.16.3.5	The Supplier must provide an Incident Report following any Priority 1 or 2 incidents within 7 calendar days. This should include, but not limited to the following detail: a) detailed description of the symptoms including error messages; b) Impact of the error; c) description of the steps taken to resolve the error; d) root cause and e) identification of any outstanding risk and improvement activities	Mandatory
6.16.3.6	The Supplier will at the request of The Authority liaise with 3rd Parties or other representatives in the course of providing the Solution (e.g. Incident Management).	Mandatory
6.16.3.7	The Supplier will support the service through active involvement in fault diagnosis and problem investigation with other Suppliers to The Authority where cause is unclear at the start of the investigation and asked to do so by The Authority.	Mandatory
6.16.3.8	The Supplier should provide a public facing web page showing the status of their service and any incidents or issues affecting it at that time.	Optional
6.16.3.9	The Supplier shall notify The Authority immediately of any losses or misuse of the data, or loss of integrity and availability of personal data. The Authority will be responsible for all communications with the Information Commissioner's Office.	Mandatory

6.16.3.10	The Supplier understands that as the Data Processor it shall be responsible for taking any action necessary to immediately notify The Authority and proactively investigate, contain and resolve any such incidents.	Mandatory
6.16.3.11	Any security incidents involving DVLA Data must be reported to a nominated contact within DVLA without undue delay and no later than 24 hours from knowledge of the incident. The information reported should include the nature of the breach, the data fields breached, the number of data subjects concerned, and action taken to date or to be taken to mitigate the risks. A full security incident report must be provided to The Authority within 5 working days of the incident. In addition, Authority and Supplier shall agree a strategy for issue resolution including key milestones.	Mandatory
6.16.3.12	Suppliers should have in place within their organisation a published fraud response plan which clearly sets out its anti-fraud policy, including fraud reporting and anti-fraud and corruption training.	Mandatory
6.16.3.13	The Supplier should provide customer level access to The Authority to their service management tool for incident reporting and tracking.	Optional

6.16.4 Change Management

6.16.4.1	The Supplier must demonstrate how they will provide a forward view to The Authority of all planned and anticipated changes.	Mandatory
6.16.4.2	The maximum amount and duration of scheduled maintenance must not exceed levels agreed with The Authority at the award stage, normally this would not exceed three hours in any calendar month.	Mandatory
6.16.4.3	Where a change is purely on The Supplier side, a minimum of 5 working days' notice must be given, unless otherwise agreed with The Authority by exception.	Mandatory
6.16.4.4	Where testing or changes will also be required to be carried out by The Authority, a minimum of three months' notice must be given to The Authority, unless otherwise agreed with The Authority by exception.	Mandatory
6.16.4.5	The Supplier must seek approval from The Authority before implementing any changes that will impact the availability or performance of the Services	Mandatory
6.16.4.6	The solution, and provider, must have the ability to update and adapt to changes in requirement as a result of customer feedback and/or other Authority requirements	Mandatory
6.16.4.7	Change requests must be responded to within 10 working days. This will include a full impact assessment unless explicitly agreed with The Authority	Mandatory
6.16.4.8	The Supplier must provide a detailed change process demonstrating how they will deliver changes to the solution in response to both Authority and industry led requirements.	Mandatory
6.16.4.9	Audited system changes by The Supplier must be recorded and available throughout the Contract Period. These must be made available to The Authority within a reasonable timescale as agreed with The Authority at the time.	Mandatory

6.16.4.10	The Supplier shall provide a test environment for The Authority and, and where integration is required with other Suppliers, to allow for production-like testing of integration and new releases, including the use of any identifiers that are in use for the production environment and to allow for penetration testing to verify the end-to-end security of the integrated and test accounts	Mandatory
6.16.4.11	The Supplier should ensure the test environment is regularly updated to replicate the production environment or forthcoming release as closely as possible	Mandatory
6.16.4.12	The Authority requires the ability to view and amend data in the test environment to facilitate execution of specific test cases. The Supplier shall detail how this would be enabled. All test data must be anonymised and not personal in nature.	Mandatory

6.16.5 Risk Management

6.16.5.1	The Supplier shall inform The Authority of new payment initiatives, mandates and/or regulations and impact assess these against these against the provision throughout the Contract Period.	Mandatory
6.16.5.2	The Supplier shall identify the risks associated with the Services, the ownership of those risks and methods of mitigating them and maintain an agreed joint operational risk register with The Authority.	Mandatory

6.16.6 Continuous Improvement

6.16.6.1	The solution, and provider, must have the ability to update the service and/or processes in a timely manner and adapt to changes in technology, legislation and industry standards and work with The Authority to implement these in accordance with the Variation Procedure.	Mandatory
6.16.6.2	The Supplier must inform The Authority of new payment innovations and methods that become available, and make such innovations and methods available in order that they can be implemented by The Authority if required in accordance with the Variation Procedure.	Mandatory
6.16.6.3	The Supplier must be able to evidence continual environmental improvements in their own organisation (ideally through an accredited EMS, i.e. ISO 14001, Green Dragon etc).	Mandatory

6.16.7 Service Management

6.16.7.1	The Supplier shall provide an appropriately qualified management team including a Contract Manager with suitable experience to manage the delivery of the Contract and ensure delivery of the Services	Mandatory
6.16.7.2	The Authority reserves the right to request an alternative Management Team Representative and Contract Manager if dissatisfied with the ones appointed to the Contract by The Supplier	Mandatory
6.16.7.3	The dedicated Contract Manager tasks shall include, but not be limited to: - • Acting as an escalation point for queries, advice and issues • Provision of proactive notification and management of issue resolution • Identification of opportunities for improvements	Mandatory

	• Trend analysis • Preparation for Service and Contract review meetings • Fulfilling requests for information from the Agencies • Information security • Risk Management	
6.16.7.4	The Contract Account Manager or equivalent shall at all times liaise closely with The Authority's key personnel. Key personnel on both sides shall be agreed and documented. Any changes should be notified as soon as possible	Mandatory
6.16.7.5	The Supplier shall make available the Contract Management Team to attend monthly service review meetings with The Authority. These reviews may be held at the DVLA offices in Swansea or via remote conferencing technology e.g. Microsoft Teams. The Authority may also request to attend Service Reviews at The Supplier's premises on occasion.	Mandatory
6.16.7.6	The Supplier shall provide to The Authority a Service Report at least 3 working days prior to the service review meeting. The content/scope of the review document is to be agreed by The Authority prior to commencement of the Contract but should include as a minimum a report of performance against all SLAs and KPIs for the review period	Mandatory
6.16.7.6	The Service review meetings shall be conducted to an agreed agenda; likely to be include but not limited to: • Performance analysis – Review of Service Report • Contractual/Operational Issues • Risk Management • Continuous Improvement • Business Continuity arrangements	Mandatory
6.16.7.7	The Supplier shall make available the Contract Management Team to attend other ad hoc or regular meetings as requested by The Authority, for example when an issue requires resolution	Mandatory
6.16.7.8	The Supplier should provide ad hoc reports on request, for example in relation to an issue	Mandatory
	Standards	
6.16.8	The Supplier must be certified against ISO/ISEC 27001 standards or equivalent	Mandatory
6.16.9	The Supplier shall keep a watchful eye on the progress of ISO20022 and if this rolls out to Direct Debits or Direct Credits during the life of the new contract, The Supplier must be compliant before this becomes mandatory for Direct Debits. More information about the ISO20022 standard can be found here https://www.iso20022.org/	Mandatory
	Invoicing	
6.16.10	The format and method of submission of invoices should be agreed between The Supplier and Authority within the first month of contract award.	Mandatory
6.16.10.1	To ensure payment, all submitted invoices should include the following detail:	Mandatory

- A valid & correct Purchase Order (PO) reference
- The name of the Contract Owner (For Attention Of)
- Detailed breakdown of charges included in the invoice, along with confirmation of any agreed discount.
- The date/period that the invoice relates to (not simply the date the document was created)
- See Section 12 for details of where to send Invoices

Mandatory

6.16.11 **Service Level Management, Criteria and Performance Measures**

6.16.11.1

Service Criteria	**Performance Measure** (Measured by Calendar Month except where noted)
Production (live) Service fully available for processing transactions over all channels	99.50%

NB Minimum acceptable availability is 99.5%, however The Authority seeks to procure a service that consistently exceeds this, and The Supplier should provide detail of their actual expected availability	Scheduled maintenance within agreed limits is excluded from this calculation.
Response time per transaction does not exceed 1 second	99% **measured daily**
365/24/7 Helpdesk Availability for P1 and P2 calls	100% Scheduled maintenance within agreed limits is excluded from this calculation.
Business hours helpdesk availability for all other calls	100% Scheduled maintenance within agreed limits is excluded from this calculation.
Helpdesk response times as agreed with The Authority	100%
Self-service portal availability	99%
BACS submission	99% within agreed timings
Batch files (if applicable to technical solution)	99% within agreed timings
Creation of mandates	99% within agreed timings
Collection of mandates	99% within agreed timings
Change requests responded to within 10 working days. This will include a full impact assessment unless explicitly agreed with The Authority	100%
Test environment availability for testing transactions over all channels	98% Scheduled maintenance within agreed limits is excluded from this calculation.

6.16.12 Service Credits

The Supplier shall provide the Services in accordance with the following Service Hours:

Online Mandate WEB Service (EVL)						
	Monday to Friday	**Saturday**	**Sunday**	**Restoration Time SLA**	**No Availability**	**Partial / Slow Availability**

					Service Credits	**Service Credits**
Platinum Service Hours	Between 08:00 and 22:00 on the last 2 Days of the Month and the first 2 days of the Month (Outside of these times Gold Service Tiers apply)			30 mins	**Redacted under FOIA section 43(2)**	**Redacted under FOIA section 43(2)**
Gold Service Hours Tier 1	07:30 to 22:00	07:30 to 17:00	07:30 to 17:00	30 mins	**Redacted under FOIA section 43(2)**	**Redacted under FOIA section 43(2)**
Gold Service Hours Tier 2	22:00 to 07:30	17:00 to 07:30	17:00 to 07:30	4 Hours	**Redacted under FOIA section 43(2)**	**Redacted under FOIA section 43(2)**

Online Mandate WEB Service (POL)						
	Monday to Friday	**Saturday**	**Sunday**	**Restoration Time SLA**	**No Availability Service Credits**	**Partial / Slow Availability Service Credits**
Platinum Service Hours	Between 08:00 and 22:00 on the last 2 Days of the Month and the first 2 days of the Month (Outside of these times Gold Service Tiers apply)			30 mins	**Redacted under FOIA section 43(2)**	**Redacted under FOIA section 43(2)**
Gold Service Hours	08:00 to 22:00	09:00 to 13:00	10:00 to 17:00	30 mins	**Redacted under FOIA section 43(2)**	**Redacted under FOIA section 43(2)**

Online Mandate Web Service (Contact Centre & Casework)						
	Monday to Friday	**Saturday**	**Sunday**	**Restoration Time SLA**	**No Availability Service Credits**	**Partial / Slow Availability Service Credits**
Gold Service Hours	07:00 to 20:00	07:00 to 17:00	n/a	30 mins	**Redacted under FOIA section 43(2)**	**Redacted under FOIA section 43(2)**

Batch Services

Batch Process Window	
Supported Days	**Monday – Sunday**
Batch Hours	18:00 – 06:00

Direct Debit and BACS Processing Services

BACS Submission Hours	
Supported Days	**Monday – Friday**
BACS Submission Hours	07:00 – 22:30

Supplier will ensure that payments are submitted to BACS on the date in which the payments are scheduled to be submitted. Any failure to submit on the scheduled day will be reported to the Buyer.
Any late processed BACS files will be treated in line with BACS processing rules. All obligations regarding BACS are KPIs only (as defined below).
End of Day batch processing should not impact the processing of online (real time) Direct Debit Services

Definitions within SLA:

"**Account Fees**" means the account fees payable by Buyer to Supplier per month.

"CC" means Contact Centre.

"**EVL**" means the Buyer's Electronic Vehicle Licensing.

"**Excluded Downtime**" means any period during which the Solution is not Available due in whole or in part to an Excluded Event.

"**Excluded Event**" means.

a) permitted system maintenance in accordance with the principles set out below;
b) the volumes in the relevant period (pro rata) being in excess of twenty-five per cent (25%) larger than the forecasted monthly volume (updated forecasts to be provided every 3 months)
c) unavailability or limited availability caused by the Buyer's systems, any third-party systems (except for Supplier Sub-Contracted Services), or the internet.
d) any Force Majeure Event or Relief Event.

e) any problem accessing the Solution due to any action on the Buyer's part that triggers a security response; or
f) Supplier being prevented or delayed from resolving an issue or incident due to an act or omission by the Buyer (including without limitation Buyer preventing Supplier from carrying out emergency maintenance by taking the Solution offline).

"**Expected Average Page Response Time**" means not greater than 3 seconds, measured within The Supplier's network. This shall exclude the contact centre's Fraud Search response time.

"**KPI**" (Key Performance Indicator) means the relevant activity represents a commitment to meet the target but does not incur any service credit.

"SLA" (Service Level Agreement) a target/metric which is binding and where The Supplier is liable for service credits.

"**Page Response Time**" means the time it takes for Supplier to make a requested page Available measured from the time the request is received at the Reference Location to the time the page is loaded at the Reference Location.

"**POL**" means the Post Office Limited, registered in England and Wales, with company number 02154540.

"**End-User**" means any person who uses the Solution for the purposes of paying, renewing or administering vehicle tax.

"**Reference Location**" means the measurement point for the measurement of Availability, Partial Availability, No Availability and Slow Availability. Reference Location shall mean a location within The Supplier's network.

"**Service Channel**" currently means POL, CC and EVL but could change at Buyer's request.

"Service Credit" means any service credit payable.

"Solution" means the EVL, POL and CC, excluding, for the avoidance of doubt, any parts referred to as being the responsibility of the Buyer or third party. (Except for Supplier Sub-Contracted Services)

1.0 Production Availability of the Solution

The Supplier will provide *ninety-nine and five tenths (99.5%)* availability of the Solution. This is a KPI. The measurement criteria tool to determine Availability shall be provided by Supplier (to be discussed and agreed with the Buyer prior to commencement of the contract). Availability will be calculated on a weekly basis but reported on a monthly basis to The Buyer.

Regular system maintenance is essential.

Planned maintenance will be performed out of service hours for POL and CC channels and at an agreed quiet time for the EVL channel and shall not exceed three (3) hours per month, unless otherwise agreed with the Buyer (such agreement not to be unreasonably withheld or delayed). Quiet Time is defined as outside of the last 5 calendar days of any month and first 3 calendar days of any month.

Emergency maintenance in relation to any Service Channel shall be dealt with in accordance with the emergency process agreed between the Parties from time to time. If the Buyer decides to decline any maintenance, then The Supplier will provide written notice of the risk of not carrying out the maintenance in advance of any event.

In such a case, the Solution shall be deemed to be Available, and meeting the Expected Average Page Response Time, during any period that the Solution is not Available, Partially Available, or there is Slow Availability, where the non-Availability, Partial Availability or Slow Availability is directly attributable to failure to perform the maintenance.
The Availability of the Solution shall be measured to determine whether there is Full, Partial or No Availability. The terms Available, Partial Availability, Slow Availability and No Availability are defined as follows:

(a) "**Available**" means that the production environment Solution is capable of being accessed at the Reference Location by all users. Availability shall be measured using The Supplier's standard measurement tools.

(b) "**Partial Availability**" means the Solution is not Available to (i) two or more of the end users, where all affected experience the same issue at the same time with the same root cause, in either case as a result of a failure located within the Reference Location.

(c) "**Slow Availability**" means, in relation to an hour of the day, the Average Page Response Time during that hour is greater than the Expected Average Page Response Time.

(d) **No Availability** means a total system failure whereby the Solution is not Available to any end- Users during the Service Hours specified in the table above.

Availability of the Solution will be measured through analysis of system logs by The Supplier, at their relevant Reference Location (not the individual Payer or End User level). If the impact differs greatly between Supplier and Buyer for the actual impact seen, then both Parties will liaise to formally review and agree the impact. All incidents will be handled via incident tickets and managed under the severity and response process described in the "Incident Management" document.

Availability is calculated on a monthly basis for each Service Channel by:

$$\frac{(\textit{time period of Availability in the measurement period}) + (\textit{Excluded Downtime in the measurement period})}{(\textit{total number of hours in the measurement period})} \times 100$$

(e) A Service Credit shall be due for each occurrence when the duration of any No Availability or Partial Availability time exceeds the "No Availability/Partial/Slow Availability service restoration time SLA" detailed in the Service Hours table above, subject always to the Monthly Service Credit Cap (as defined below)

(f) A single Partial Availability Service Credit shall apply for each hour beyond the "No Availability/Partial Availability service restoration time SLA" detailed in the Service Hours table above when there is Slow Availability, except where such Slow Availability has been caused in whole or in part by an Excluded Event, and subject always to the Monthly Slow Availability Service Credit Sub-cap (as defined below).

(g) Where a period of No Availability, Partial Availability, or Slow Availability spans more than one Service Channel.

i) and Service Credits are payable (because the restoration time SLA has been exceeded), the Service Credit applicable to the relevant Service Hour period shall apply (so that different service credit amounts may apply).
For example, if a period of No Availability affecting the EVL Service Channel occurs at 21:30 on the last Monday of the month (during Platinum Service Hours), and Supplier fails to restore Availability by 22:00, the Service Credit payable would be £8,000. If Supplier then fails to restore Availability in the next 4 hours, the next Service Credit payable would be £1,000 (as the Service Hour period has changed from Platinum to Gold Tier 2);

ii) the "No Availability/Partial Availability service restoration time SLA shall be adjusted accordingly. For example, if a period of No Availability affecting the EVL Service Channel occurs at 21:30 on a regular Monday (i.e. during Gold Service Hours), and Supplier fails to restore Availability within 30 minutes, a Service Credit of £1,000 would be payable. The time SLA then moves to 4 hours, and the next Service Credit would then only become payable 4 hours and 30 minutes after the period of No Availability first started.

(h) Where the No Availability/Partial Availability service restoration time SLA spans more than one Service Hour Period, the restoration time and any Service Credit payable shall be pro-rated. For example, if a period of No Availability affecting the EVL Service Channel occurs at 21:45pm on the last Monday of the month (during Platinum Service Hours), and Supplier fails to restore Availability within 30 minutes, the Service Credit payable shall be pro-rated. The Service Credit regime has changed during the life of the incident as the incident has moved between Platinum and Gold Tier 2.

(i) The Buyer may request that the Solution continues to meet the SLAs/KPIs during periods of high demand. The Buyer will notify The Supplier of any anticipated periods of high demand when providing the forecasts to The Supplier. The Parties shall agree any changes to the Services that may be reasonably required to deal the additional demand, such changes to be handled in accordance with the Change Control Procedure.

(j) The aggregate Service Credits payable in any month ("**Monthly Service Credit Cap**") shall not exceed 20% of the invoice for that month:

(k) Service Credits apply to No Availability/Partial Availability and Slow Availability SLAs. More than one Service Credit will not be paid for the same incident. Where an incident impacts more than one Service Channel, only the larger or largest Service Credit applies. Where the same incident triggers more than one Service Credit (for example Partial/No Availability and Slow Availability), only the largest Service Credit will be payable.

For other multiple incidents with the same root cause The Supplier will be liable for Service Credits for each incident unless either of the following applies:

1) Where The Supplier has implemented a Workaround, which has been agreed in writing with the Buyer (such agreement not to be unreasonably withheld or delayed) that provides an acceptable level of functionality to the Buyer, then the second and subsequent service credits will be suspended for a period of time to be agreed with the Buyer.

2) Where a fix has been identified by The Supplier and the Buyer requests that the implementation of the fix is delayed, then the second and subsequent service credits will be suspended, and the permitted restoration time extended until The Supplier receives approval to proceed with the implementation of the fix.

(l) Examples:

1. if the Solution had No Availability for 31 minutes outside of the Platinum+ peak periods during tier 1 Service Hour then a credit of would be payable. If the duration of the No Availability breach continued then a further payment would be due for every subsequent 30 minutes, subject always to the Monthly Service Credit Cap.

2. If the Solution had Average Page Response Times greater than the Expected Average Page Response Time for two hours during a Gold period and a call is logged with Supplier about the same issue during the period of Slow Availability in accordance with the procedures in this Service Level Schedule, then two Slow Availability service credits will have occurred and are payable, subject always to the Monthly Service Credit Cap.

2.0 Monitoring for Availability and Response Times

Supplier will provide application monitoring tools to monitor the Reference Locations and report on the Availability and response times of the Solution.

Web availability testing will be done every 1 minute. All monitoring and reporting are part of the Solution fees paid for by the Buyer. All such measurements are SLAs.

This SLA shall not apply until 90 days after the Start Date.

3.0 Page Response times

3.1 **Hourly Average Response Time**
The Supplier shall report the hourly Average Page Response Time.

Note: Response times spikes that occur during an hourly period where the hourly transaction volumes exceed the volumes provided by the Buyer will be excluded from this calculation and service credits.

3.2 **Monthly Average Response Time**
The Supplier shall report the monthly Average Page Response Time as a KPI only. Service Credits are not payable for a failure to meet the monthly Average Page Response Time.

4.0 Service Level Review

The Buyer and supplier will review the service level commitments monthly or as needed in relation to service level failures or severity 1s.

INCIDENT REPORTING	SEVERITY	CHANNEL	CALL ANSWER TIME	SUPPLIER RESPONSE	SUPPLIER UPDATE FREQUENCY (unless otherwise agreed by the Buyer's Service Level Manager or Incident Manager)
Client has fulfilled Client Responsibilities	1	Phone	<2 minutes	5 minutes	Every 30 minutes
	2	Phone	<2 minutes	5 minutes	Every 60 minutes
	3	Phone / Email		Within 24 Hours	Every 24 hours
	4	Email		Within 24 Hours	Every Week
	5	Email		Within 2 days	Every Week

In relation to Severity 1 and Severity 2 incidents only, repeated failure (more than 1 per quarter) to meet the above Incident Management service measures shall result in a single Service Credit of **Redacted under FOIA section 43(2)** to be applied. For the avoidance of doubt, the Service Credit would only apply to each incident/ticket raised through the Incident Reporting procedure.

7. Social Value Considerations

Evaluation of the social value aspect of bids will ensure all potential suppliers, including SMEs, VCSEs and those new to government business, can successfully bid by describing what they will deliver and how they will deliver it (i.e. it is the quality of what is being offered that will count in the evaluation, not the quantity).

It is a legal obligation under the Bribery act of 2010 that commercial organisations must demonstrate that they have in place relevant procedures including training, to

prevent bribery. Any organisation failing to do so, where a bribery case is identified and prosecuted, the organisation can be held liable. The Bribery response plan of any potential supplier must be available to The Authority upon request and in line with the Bribery Act 2010.

In accordance with Government Guidance, The Authority will apply a minimum of 10% to the evaluation process for Social Value considerations within a bid. There is one common theme in the Finance and Insurance industry that align to the Social Value model:

- Tackle workforce inequality

The successful supplier will demonstrate how they deliver social benefits that support key social outcomes that are highlighted in the table below.

Theme	**Policy Outcome**	**Delivery Objective – What good looks like**
Equal opportunity	Tackle workforce inequality	Activities that: - Demonstrate action to identify and tackle inequality in employment, skills and pay in the contract workforce.

These aspects will be evaluated as part of the tender process along with any sustainability requirements identified and outlined within this document.

Social Value KPIs

Progress on social value measures will be discussed and reported on as part of contract review meetings and the strategic supplier forum.

Key Performance Indicator	Measurement
MAC 6.1: Demonstrate action to identify and tackle inequality in employment, skills and pay in the contract workforce	Report monthly on current position and produce a progress plan towards maintaining or increasing- • Total percentage of full-time equivalent (FTE) people from groups Under-represented in the workforce employed under the contract, as a proportion of the total FTE contract workforce, by UK region. Report monthly on current position and produce a progress plan towards decreasing- • Mean percentage of the gender pay gap of full-time equivalent (FTE) people employed under the contract, as a proportion of the total FTE contract workforce, within the Finance and Insurance industry. Report monthly on current position and produce a progress plan towards maintaining or increasing- • Number of people from groups Under-represented in the workforce offered training schemes under the contract, by UK region.

7.1 Modern Slavery Considerations

7.1.2 Modern Slavery Assessment Tool (MSAT)

The MSAT is a modern slavery risk identification and management tool. This tool has been designed to help public sector organisations work in partnership with suppliers to improve protections and reduce the risk of exploitation of workers in their supply chains. It also aims to help public sector organisations understand where there may be risks of modern slavery in the supply chains of goods and services they have procured.

Please note that the successful tenderer, as part of the contract, may be requested to complete the MSAT and, where appropriate, work with the DVLA in resolving any issues identified. If completion of the MSAT is required, the Commercial Advisor identified in Section 15 will instruct as appropriate. Suppliers who have previously completed the MSAT for another Government body may share their results with The Authority.

The requirement to complete and assess the MSAT at appropriate intervals throughout the Contract Period may also form part of the Contract Management process.

In addition to completing the MSAT, and depending on the outcome of this assessment, it may be necessary for the DVLA to work with the successful supplier to undertake a supply chain mapping exercise to have a more informed position of any modern slavery risks within the wider supply chain beyond first tier/prime supplier. Such an exercise may also cover wider compliance with all relevant social, ethical and legal requirements of first tier/prime Suppliers and their supply chain.

For further information on the MSAT and registration process, please visit: https://supplierregistration.cabinetoffice.gov.uk/msat

7.2 Prompt Payment

The Government understands the importance of prompt, fair and effective payment in all businesses. Being paid promptly for work done ensures businesses have a healthy cash flow.
The Supplier must have systems in place to pay those in their supply chain promptly and effectively, i.e. within your agreed contractual terms. The Supplier shall have procedures for resolving disputed invoices with those in your supply chain promptly and effectively.

7.3 Supply Chain Visibility

The Government wants to level the playing field and increase the visibility of supply chain opportunities to assist suppliers, including SMEs, in bidding for work in its supply chains. Procurement Policy Note (PPN) 01/18 sets out the requirement for successful suppliers of in-scope procurements to advertise subcontracting opportunities and report on how much they spend with Small/Medium Enterprises (SME) and Voluntary, Community and Social Enterprises (VCSE). This requirement is in scope of this PPN and requires the successful prime supplier(s) to:

a) advertise on Contracts Finder, subcontract opportunities arising from that contract above a minimum subcontract threshold of £25,000; and

b) separately, report on how much they spend on subcontracting, and separately how much they spend directly with SME or VCSE organisations in the delivery of the original contract.

The contracted Supplier will be required to fulfil the reporting requirements as set out in the PPN and the Terms and Conditions of this requirement.

7.4 Sourcing Playbook Considerations

- DVLA has been using DD for payment processing since 2014, internal knowledge and experience across the respective stakeholder community is (reasonably) well-developed and the supply market is mature and well

regulated (arguably evolving at pace given the innovation being driven by Fintech entrants).

- This is a re-procurement of an existing Service, so a trial is not appropriate in the circumstances.

KPI:

- We have drafted a number of KPI's that are relevant and proportionate to the size and complexity of the requirement, align with the intended benefits and complement the service level agreement (and service credit) regime.
- These range across financial, customer, process and people and are designed to be both SMART and easily understood.

Economic and Financial Standing (EFS):

- The criterion is set out in the respective Standard Supplier Questionnaire (SSQ) and is intended to identify the bidders' financial capacity to perform the contract at the outset. This also incorporates annual (and where appropriate / relevant periodic) testing against agreed measurement criteria to identify any change in the risk profile that might highlight any financial stress.
- We consider these to be proportionate to the size and nature of the contract and not overly risk averse.
- All bidders, regardless of size and organisational structure will be treated fairly and will not be inadvertently disadvantaged by these financial assessment measurements.

Resolution Planning:

- We will be using the Cabinet Office Mid-tier Contract for DD which contains standard clauses setting out the steps to deal with resolution planning and evaluation.

7.5 Net Zero Carbon Reduction Plans

The UK Government amended the Climate Change Act 2008 in 2019 by introducing a target of at least a 100% reduction in the net UK carbon account (i.e. reduction of greenhouse gas emissions, compared to 1990 levels) by 2050. This is otherwise known as the 'Net Zero' target. Procurement Policy Note (PPN) 06/21 sets out how contracting authorities should take account of Suppliers' Net Zero Carbon Reduction Plans in the procurement of major Government contracts and this requirement is in scope of this PPN.

See Section 14 ("Evaluation Criteria") and the above PPN for full details.

7.6 Transparency/Publication of Key Performance Indicators (KPIs)

In accordance with the UK Government's transparency agenda, to build trust and increase transparency in the delivery of public services, DVLA are required to publish and make publicly available key supplier performance data from our most important contracts. This contract has been classified as one of DVLA's most

important contracts therefore **three** Key Performance Indicators (KPIs), which are representative of the general purpose of this contract, will be selected for publication on a quarterly basis.

KPIs and Thresholds

It is our firm intention to fully engage with the contracted Supplier to select the **three** KPIs and obtain written approval for their initial publication and in perpetuity thereafter for each quarter.

The selected KPIs will clearly relate to the contractual requirements and will be based on SMART criteria, i.e. they will be Specific, Measurable, Achievable, Relevant and Time-bound. Each KPI will have clearly defined descriptions and target performance thresholds set by the DVLA, in consultation with The Supplier, at the outset of the contract.

Supplier performance against the target thresholds will be rated as one of the following for the purposes of publication.

- **Good**: The Supplier is meeting or exceeding the KPI targets that are set out within the contract.
- **Approaching Target**: The Supplier is close to meeting the KPI targets that are set out within the contract.
- **Requires Improvement**: The performance of The Supplier is below that of the KPIs targets that are set out within the contract.
- **Inadequate**: The performance of The Supplier is significantly below that of the KPIs targets that are set out within the contract.

Where will DVLA Publish the KPIs?

The three selected KPIs and associated ratings above will be published on GOV.UK on a quarterly basis.

Note: You are requested to acknowledge your understanding and acceptance of these shared obligations, under the government's transparency agenda, in your tender.

8. Quality Assurance Requirements

Suppliers must conform to all BACS rules and procedures as detailed in the Service User's Guide and rules to the DD Scheme and to DD operational rules, file submission criteria and associated submission documentation.
http://www.bacs.co.uk/bacs/sugr/pages/serviceusersguide.aspx

Bidders are expected to provide evidence/certificates of pertinent standards as part of their bid. The standards and/or certificates will need to be checked and validated at appropriate intervals for the duration of the contract.

9. Other Requirements

9.1 Information Assurance

IAG Security Schedule

Where The Supplier processes Government data, including but not limited to, personal data on behalf of the DVLA the following requirements shall apply, unless otherwise specified or agreed in writing.

Assurance and Audit

- **Statement of Assurance**
  This contract will require The Supplier to process government data on DVLA's behalf. The successful tenderer will be required to complete a Statement of Assurance Questionnaire (SoAQ) prior to formal contract award and before any processing of data commences in relation to this contract, to satisfy DVLA that its data will be appropriately protected. The purpose of the questionnaire is to assess the maturity of policies, systems and controls associated with the handling of our data.

  As part of this, The Supplier must confirm how DVLA data or information will be securely managed at each stage of the supply chain, including any sub-contractors, sub-processors or any other third parties.

  The questionnaire must be completed and returned prior to contract award, and annually thereafter, and will be assessed by our Information Assurance & Governance team. DVLA will work with The Supplier to address any information aspects requiring improvement.

- **Audits of Processing**
  The Supplier shall allow for auditing of its DVLA data processing activity. Such audits will be conducted by the DVLA, the DVLA's representative or an agent acting on DVLA's behalf and may include a site visit to The Supplier's offices where DVLA data is processed.

- **Monitoring**
  The Supplier shall collect audit records which relate to all events in delivery of the service or that would support the analysis of potential and actual compromises resulting in a breach of security or a data loss event.

  In order to facilitate effective monitoring and forensic readiness such audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the service, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of DVLA data. The retention periods for audit records and event logs must be agreed with the DVLA and documented.

- **Data Protection Impact Assessment**
  Where this contract involves the processing of personal data on behalf of DVLA that results in a significant risk to the rights and freedoms of individuals, The Supplier shall

provide all reasonable assistance to DVLA in the preparation and completion of a Data Protection Impact Assessment (DPIA) prior to commencing any processing of personal data. A DPIA may be required prior to award or during the term of the contract if the risk profile changes.

Such assistance may, at the discretion of the DVLA, include:

(a) a systematic description of the envisaged processing operations and the purpose of the processing;
(b) an assessment of the necessity and proportionality of the processing operations in relation to the services;
(c) an assessment of the risks to the rights and freedoms of data subjects; and
(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data.

Certification

The Supplier shall ensure they hold relevant certifications in the protection of personal data and/or evidencing the effectiveness of technical and organisational measures they have in place. These certifications must be maintained throughout the entirety of the contract, including any applicable extension periods. Evidence of valid certificates and corresponding documentation shall be provided upon request by the DVLA's representative or an agent acting on DVLA's behalf.

Supplier Devices

- **Removable Media**
  The Supplier shall not use removable media in the delivery of this contract without the prior written consent of the DVLA.

- **Mobile Device Management**
  The Supplier shall ensure that any DVLA data which resides on a mobile, removable or physically uncontrolled device is stored encrypted, using a product or system component which has been formally assured through a recognised certification process agreed with the DVLA, except where the DVLA has given prior written agreement to an alternative arrangement.

- **Security**
  The Supplier shall ensure that any device which is used to process DVLA data meets all of the security requirements set out in the National Cyber Security Centre's End User Devices Platform Security Guidance, a copy of which can be found at https:www.ncsc.gov.uk/guidance/end-user-device-security.

Governance

- **Organisational Structure**
  The Supplier shall have a senior individual responsible for DVLA assets within your custody.

- **Asset Management**
  The Supplier shall implement and maintain an asset register that identifies and records the value of sensitive DVLA assets which require protection. This includes both physical and information assets. Risk assessments should be managed to

ensure that the security of the asset is proportionate to the risk depending on value and sensitivity.

- **Policies**
  The Supplier shall establish, or indicate that they have in place, policies which detail how DVLA assets should be processed, handled, copied, stored, transmitted, destroyed and/or returned. These shall be regularly maintained. The Supplier shall provide evidence of relevant policies upon request.

- **Risk Assessment**
  - **Technical**
    The Supplier shall perform a technical information risk assessment on the service/s supplied and be able to demonstrate what controls are in place to address any identified risks.
  - **Security**
    The Supplier shall ensure an annual security risk assessment is performed at any sites used to process or store any DVLA data. This assessment must include perimeter security, access controls, manned guarding, incoming mail and delivery screening, secure areas and/or cabinets for the storage of sensitive assets and have a demonstrable regime in place for testing controls against operational requirements.

- **Return of Data / Information to DVLA**
  The Supplier must be able to demonstrate they can supply a copy of all data or information on request or at termination of the service.

- **Destruction / Deletion of Data or Information**
  The Supplier must be able to securely erase or destroy all DVLA-related data or information that it has been stored and processed for the service, upon DVLA request.

- **Incident Management**
  The Supplier shall have policies in place which set out how information security incidents, and personal data breaches or data loss events (including breaches to the confidentiality, integrity, availability, and resilience of data) should be managed and who it should be escalated to, including notifying the DVLA immediately, or in any case within 24 hours, of becoming aware of the incident/s and/or breach/es.

  This policy shall also include:
  a) individual responsibilities for identifying and reporting security incidents and information security breaches;
  b) a reporting matrix including escalation points;
  c) an up-to-date list of relevant internal and external contact points; and
  d) a timeline detailing at which point the policy should be implemented.

Personal Data

- **Processing Personal Data**
  The Supplier as part of the contract agrees to comply with all applicable UK law relating to the processing of personal data and privacy, including but not limited to

the UK GDPR and the Data Protection Act 2018, and the EU GDPR where applicable to the processing.

- **DVLA Written Processing Instructions**
  The Supplier shall comply with DVLA's written instructions, as outlined in the 'Schedule of Processing' in the contract.

- **International Transfers (Offshoring) of Government Data**
  When international transfers or offshoring is described, the focus is typically on the physical location where data is hosted (such as where the data centres are located). However, whilst physical location of data is a critical part of the offshoring question, it is important to understand how and where data might be logically accessed. Administrators or technical support staff may be located anywhere in the world, with logical access to data.

  The Supplier (and any of its third-party sub-contractors, sub-processors or suppliers) shall not, transfer, store, process, access or view DVLA data outside of the UK without the prior written approval of DVLA, which may be subject to conditions. Any changes to offshoring arrangements must also be approved by DVLA.

  Any request to offshore DVLA data must receive formal approval from DVLA prior to the commencement of any data processing activity. This is requested through the completion of DVLA's offshoring questionnaire.

  In the event that The Supplier proposes to offshore any DVLA data as part of the contract, they would be required to provide details in the offshoring questionnaire about the processing to be carried out offshore, including:
  a) the privacy risks and the security controls in place to protect the data;
  b) how the offshoring arrangement is legitimised to comply with relevant data protection legislation (e.g. adequacy decision, appropriate safeguards, Standard Contractual Clauses/International Data Transfer Agreements); and
  c) where applicable details of any transfer risk assessment that has been conducted, along with any supplementary measures implemented.

Processing of Sensitive Information (not Personal Data)

- **Security Classification of Information**
  If the provision of the services requires The Supplier to process DVLA data which is classified as OFFICIAL: SENSITIVE or higher, The Supplier shall implement such additional measures as agreed with the DVLA in order to enhance the safeguarding of such information. A copy of the Government Security Classification scheme can be found at:
  https://www.gov.uk/government/publications/government-security-classifications

Personnel

- **Security Clearance**

  - **Level 1**
    The Supplier is required to acknowledge in their response that any supplier staff that will have access to the DVLA site for meetings and similar (but have no access to the DVLA systems), must be supervised at all times by DVLA staff.

  - **Level 2**
    The Supplier is required to confirm that Baseline Personnel Security Standard clearance (BPSS) is held for any supplier staff that will have:
    - access to or will process DVLA (customer or staff) data or information.
    - access to the DVLA site to provide routine maintenance.
    - access to the DVLA site and DVLA systems

    The BPSS comprises verification of the following four main elements:
    1. Identity;
    2. Employment History (past 3 years);
    3. Nationality and Immigration Status;
    4. Criminal Record Check (unspent convictions only).

    The aim of the BPSS verification process is to provide an appropriate level of assurance as to the trustworthiness, integrity and proper reliability of prospective staff. The Supplier is required to provide evidence of relevant supplier staff clearance in their response.

  - **Level 3**
    The Supplier is required to confirm in their response that any supplier staff that have access to the DVLA site and DVLA systems, administration rights, sensitive programmes or large blocks of sensitive data or information must have full 'Security Check' (SC) clearance.

- **Employment Contracts**
  The Supplier shall confirm that organisational and individual responsibilities for information security are clearly defined in the terms and conditions of employment contracts, along with relevant non-disclosure agreements, where the individual with have access to any DVLA data, information and /or the DVLA site or systems.

- **Training**
  The Supplier shall maintain a mechanism to ensure employees and contractors receive appropriate information security awareness and data protection training upon appointment, and perform regular updates to organisational policies and procedures, as relevant for each job function. Evidence must be provided where reasonably requested by DVLA.

- **Access Rights**
  The Supplier shall ensure their staff are provided only the necessary level of access (using the principle of least privilege) to DVLA data or information, to deliver their job function within the contracted service(s).

Upon staff migration, or termination of employment, The Supplier shall verify that there is a process in place to ensure assets are returned and rights to assets revoked without undue delay.

Evidence of the above must be provided where reasonably requested by DVLA.

Business Continuity and Disaster Recovery
The Supplier shall have business continuity and disaster recovery plans in place to maintain or quickly resume any services provided to DVLA and shall maintain compliance with relevant legislation.

Data Sharing
DVLA's Contract Owner will work with the successful tenderer to implement any information sharing or data sharing procedures and associated DVLA requirements that may be needed at any point during the Contract Period.

Information or data sharing procedures will need to be formally assessed and approved by DVLA through the Data Sharing Clearance Process, managed by the Information Assurance & Governance Team.

The Supplier will submit any requirements for information / data sharing via the Contract Owner to the DVLA who will consider the changes through this Data Sharing Clearance process. Any proposals shall be considered and if approved an implementation plan will be formally offered to and accepted by both the DVLA and The Supplier before commencement.

This approvals process is designed to assess and identify additional measures and safeguards that may be required to protect data to those already stated in this specification document.

9.2 Cyber Security

The Government has developed Cyber Essentials, in consultation with industry, to mitigate the risk from common internet-based threats.

It will be mandatory for new Central Government contracts, which feature characteristics involving the handling of personal data and ICT systems designed to store or process data at the OFFICIAL level of the Government Security Classifications scheme (link below), to comply with Cyber Essentials.
https://www.gov.uk/government/publications/government-security-classifications
All potential tenderers for Central Government contracts, featuring the above characteristics, should make themselves aware of Cyber Essentials and the requirements for the appropriate level of certification. The link below to the Gov.uk website provides further information:
https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
As this requirement features the above characteristics, you are required to demonstrate in your response that:

- Your organisation has Cyber Essentials (preferably CE+) certification; **or**

- Your organisation will be able to secure Cyber Essentials (or preferably CE+) certification prior to commencement of the required services/deliverables; **or**
- Your organisation has other evidence to support that you have appropriate technical and organisational measures to mitigate the risk from common internet-based threats in respect to the following five technical areas:
  - Boundary firewalls and internet gateways
  - Secure configuration
  - Access control
  - Malware protection
  - Patch management

The successful tenderer will be required to provide evidence of Cyber Essentials (or CE+) certification 'or equivalent' (i.e. demonstrate they meet the five technical areas the Cyber Essentials Scheme covers) prior to commencement of the required Services/Deliverables. This will be through the completion of the Statement of Assurance Questionnaire (SoAQ).

The successful tenderer will be required to secure and provide evidence of Cyber Essentials (or CE+) re-certification 'or equivalent' (i.e. demonstrate they meet the five technical areas) on an annual basis.

Further information regarding the certification process can be found here:
https://www.ncsc.gov.uk/cyberessentials/overview

9.3 Data Sharing

DVLA's Contract Owner will work with the successful tenderer to implement any information sharing or data sharing procedures and associated DVLA requirements that may be needed at any point during the Contract Period.

Information or data sharing procedures will need to be formally assessed and approved by DVLA through the Data Sharing Clearance Process, managed by the Data Sharing Strategy & Compliance team (DSSC).

The Supplier will submit any requirements for information / data sharing via the Contract Owner to the DVLA who will consider the changes through this Data Sharing Clearance process. Any proposals shall be considered and if approved an implementation plan will be formally offered to and accepted by both the DVLA and The Supplier before commencement.

This approvals process is designed to assess and identify additional measures and safeguards that may be required to protect data to those already stated in this specification document.

9.4 Sustainability

The DVLA is committed to reducing any negative impacts produced by our activities, products and services. This aligns with the Greening Government

Commitments which state we must: “Continue to buy more sustainable and efficient products and services with the aim of achieving the best long-term, overall value for money for society.”

DVLA is certified to ISO 14001:2015 and more information is available in our Environmental Policy at: https://www.gov.uk/government/publications/dvlas-environmental-policy The supplier shall comply with this policy.

Where appropriate, The Supplier shall assist DVLA in achieving its Greening Government Commitments, current iteration detailed on Greening Government Commitments 2021 to 2025 - GOV.UK (www.gov.uk) i.e. Reduce CO_2 emissions through energy consumption and travel, reduce water consumption and waste produced.

The Supplier shall provide the specified services without the use of single use plastic in line with Government commitments.

The Supplier shall be able to evidence continual environmental improvements in their own organisation (ideally through a certified EMS, i.e. ISO 14001, Green Dragon etc).

If available, The Supplier shall provide the Buyer with a copy of their sustainability or environmental policy.

The Supplier shall ensure that its own supply chain does not have negative environmental or social impacts.

If requested, The Supplier shall be able to provide data on carbon emissions related to the services being supplied to aid with scope 3 emission calculations and other Government reporting requirements.

The Supplier shall promote resource efficiency and waste avoidance, to reduce waste arising and consumption of natural resources. Any waste shall be disposed of in accordance with the waste hierarchy (as per the Waste (England and Wales) Regulations 2011) and duty of care (as per the Environmental Protection Act 1990 and the Environmental Protection (Duty of Care) Regulations 1991).

The Supplier shall continually aim to travel sustainably between sites whilst conducting DVLA business and attending DVLA sites.

The Supplier shall be committed to reducing their carbon emissions year on year.

The Supplier shall ensure that any activities conform to overarching principles in the Greening Government ICT and Digital Services Strategy, current iteration detailed on https://www.gov.uk/government/publications/greening-government-ict-and-digital-services-strategy-2020-2025/greening-government-ict-and-digital-services-strategy-2020-2025. This strategy outlines the Government’s vision to be a global leader in sustainable ICT. The Supplier must confirm their understanding and acceptance of the strategy.

9.5 Health and Safety

DVLA has an Occupational Health and Safety Management System that is certificated to ISO45001. Further information on our Health & Safety Policy, is available on request from the Commercial Advisor. (See Section 15 for Points of Contact):

All Supplier Staff working in the DVLA on any of our premises must fully comply with relevant health and safety legislation, together with health, safety and welfare policy and management arrangements applied by the DVLA. If appropriate, these issues must be addressed at or before the award of the contract and may form part of the procurement process. Where requested, Suppliers will be required to provide copies of their health and safety policy statement, risk assessments and method statements, clearly identifying any safety implications that their activities may have and how these will be managed. Contract management staff are responsible for checking health and safety information provided by Suppliers and passing relevant information to local line management and staff. Supplier's safety performance will be monitored and checked as part of normal contract management.

Tenderers should:

- Have an appointed competent person responsible for H&S, details to be made available to DVLA on request.
- Have emergency arrangements and plans for their goods/product/service, and observe DVLA's arrangements whilst on site, or through the course of the business or contract.
- Have adequate provision for your own first aid when on site.
- Have an accident reporting and recording process for all near miss, accidents/incidents, or violent and aggressive behaviours. Any incident on DVLA site should be reported immediately to the DVLA's Health and Safety Team
- Communicate with DVLA on any health and safety matter or issue in relation to the contract/product/supply of goods or service, notifying DVLA of any Health and Safety hazard, which may arise in connection with its supply of goods, products, or services.
- Indemnify DVLA in the instance where failure of the company's product/service, acts or omissions, with regards to health and safety, results in an economic penalty, time delay, issue, accident/incident or claim against the DVLA.
- Have suitable and sufficient insurance cover for all business/products/services supplied/that are provided to DVLA.
- Have documented, suitable and sufficient, risk assessments and method statements, covering all significant activities and deliveries of products, goods and services. Copies to be made available to DVLA on request.
- Provide suitable and sufficient health and safety training, information and instruction for all its employees/contractors/subcontractors. Records to be made available on request.

- Engage with DVLA's Security/Estates Management Group to arrange access to all DVLA premises/buildings.
- Comply with all vehicle and driver legal requirements and DVLA policies whilst driving on premises or conducting business for DVLA

9.6 Estates

DVLA Estates Management Group stipulate that where appropriate, the following must be adhered to:

- Should new equipment need to be delivered - All deliveries/removal of equipment to/from site are in line with The Authority security procedures.
- Should attendance to site need to be required - All contractors are booked in via the pass offices and adhere to the pass off procedures.

9.7 Diversity and Inclusion

The Public Sector Equality Duty (PSED) is a legal requirement under the Equality Act 2010. The Equality Duty ensures that all public bodies play their part in making society fairer by tackling discrimination and providing equality of opportunity for all. It ensures that public bodies consider the needs of all individuals in their day-to-day work – in shaping policy, in delivering services, and in relation to their own employees. DVLA is committed to encouraging equality, diversity and inclusion within our workforce and against unlawful discrimination of employees, customers and the public. We promote dignity and respect for all, and we will not tolerate, bullying harassment or discrimination by staff, customers or partners we work with. Everyone working for us and with us, as partners in delivering our services, has a personal responsibility for implementing and promoting these policy principles in their day- to-day transactions with customers and our staff.

A full copy of our Equality, Diversity and Inclusion Policy is available on request from the DVLA.

9.8 Business Continuity

As this is a high criticality contract there are the following requirements from Business Continuity:

- Suppliers shall have robust Business Continuity and Disaster Recovery Plans which align to a code of practice such as ISO22301. Suppliers must supply the contents of these plans to The Authority.
- The successful supplier will test their business continuity arrangements no less than once per annum and shall inform The Authority when such tests or exercises are scheduled. Outcomes of these tests or exercises must be made available to The Authority in writing upon request.
- Suppliers will notify The Authority in writing within twenty-four (24) hours of any activation of the business continuity plan, in relation to the services provided to The Authority.

9.9 Use of DVLA Brands, Logos and Trademarks

The DVLA does not grant the successful Supplier licence to use any of the DVLA's brands, logos or trademarks except for use in communications or official contract documentation, which is exchanged between the DVLA and the successful Supplier as part of their fulfilment of the Contract.

Approval for any further specific use of the DVLA's brands, logos or trademarks must be requested and obtained in writing from the DVLA.

9.10 Welsh Language Scheme Requirements

The contract will require the contracted Supplier to deliver services to the public in Wales, on behalf of the DVLA. Consequently, the requirements of the Welsh Language Scheme (Annex 2) will apply.

10. Management and Contract Administration

Prospective Suppliers are required to provide details of their account management structure in respect of the Agreement and of how they propose to manage independent contracts such as with subcontractor(s)

Prospective Suppliers must detail their escalation/complaints procedure and relevant timescales required to resolve any complaints.

Prior to the commencement of each contract, The Supplier will provide details of the senior managers responsible for the contract, account managers, day to day contacts and any other key staff and supported by details of their previous experience.

The Parties shall appoint the following key personnel as a minimum and shall provide each other with up-to-date contact details for each throughout the Contract Term:

Role	**Personnel of**	**Point of contact for**
Contract Owner	Authority	• Day-to-day Service delivery and performance. • Escalation of operational issues.
Account Manager	Supplier	
Commercial Advisor	Authority	• Contractual queries or changes. • Escalation of contractual issues.
Commercial Manager	Supplier	• Contractual queries or changes. • Escalation of contractual issues.

Data Protection Officer	Supplier	• Discussion of security controls protecting The Authority's information in this service • Contact point for Data Incidents

A Supplier representative shall be available to provide support to The Authority on operational and financial queries Monday – Friday during The Authority's working hours of 08:00 – 17.00 (excluding Bank Holidays) and must offer the option of wider support hours if required.

The Supplier shall appoint a Contract Account Manager and tasks shall include, but not be limited to:

- Acting as an escalation point for queries, advice and issues;
- Identification of opportunities for improvements;
- Informing The Authority of new risks;
- Trend analysis;
- Preparation for Contract review meetings;
- Fulfilling requests for information from The Authority;
- Information security.

The Suppliers Contract Account Manager shall also be responsible for liaison with The Authority's key Operational Management team, the Contract Owner, and the Commercial Advisor. In addition, they shall attend implementation meetings, as requested by The Authority.

After Contract commencement The Supplier shall attend performance meetings at The Authority's premises or participate remotely via teleconferences to review the progress of the contract, to discuss the management information and to review any problems that may have arisen in the preceding period. The frequency of these meetings is to be confirmed but will be at least monthly. In the event that issues are identified, flexibility is required, and ad hoc meetings maybe scheduled between The Authority and The Supplier

These Contract performance review meetings will be conducted to an agreed agenda; the following elements are likely to be included:

- Performance analysis – Review of SLAs and KPIs
- Contractual/Operational Issues
- Compliance and satisfaction levels
- Business Continuity issues and updates
- Proposals for improvements on any area of the contract
- Financial stability
- Review of risk assessment
- Provide updates on any new security threats identified, including threats to personal data.
- Any future relevant legislation changes
- Progress on Social Value criteria

Any issues or queries raised by The Authority during the term of the contract will be logged and resolved within two Working Days. Anything that cannot be resolved within this timeframe will be escalated for discussion at service review meetings.

The Supplier shall prepare and maintain a contract and operational risk register in accordance with Authority's instructions. The Supplier shall identify risks, allocate risk mitigation action and ownership, and report to The Authority on progress on mitigation at applicable risk review meetings to be agreed between The Supplier and The Authority.

The Supplier shall advise The Authority immediately of any material issues which it would reasonably expect may generate complaints or receive regulatory or press attention.

The Supplier is administering this contract on behalf of DVLA and will be subject to pay service credits to The Authority when responsible for the loss of Vehicle Excise Duty resulting from service failures/issues within the Service Supplier system.

The Supplier shall ensure fully robust staffing and disciplinary procedures are in place and are applied for all Supplier personnel. The Supplier shall ensure their Staff operatives are fully trained in all relevant areas.

The Authority receiving services from The Supplier will require designated staff that will be responsible for the contract management and service review for their element of that contract.

The Authority will agree performance review meetings with The Supplier as part of the initiation of the respective contract.

Sub-contracting to Small and Medium Enterprises (SMEs):

DfT is committed to removing barriers to SME participation in its contracts, and would like to also actively encourage its larger suppliers to make their sub-contacts accessible to smaller companies and implement SME-friendly policies in their supply-chains (see the Gov.Uk website for further information).

To help us measure the volume of business we do with SMEs, our Form of Tender document asks about the size of your own organisation and those in your supply chain.

If you tell us you are likely to sub-contract to SMEs, and are awarded this contract, we will send you a short questionnaire asking for further information. This data will help us contribute towards Government targets on the use of SMEs. We may also publish success stories and examples of good practice.

11. Training / Skills / Knowledge Transfer

The Supplier shall provide training and support on the use of their products, services and tools, and provide or organise training and support of any applicable subcontractors' products, services and tools to The Authority.

The Supplier shall deliver any training required to The Authority in readiness for the “go live” date. This shall include the issue of user guides, training materials, communications, and any applicable access to The Suppliers system to The Authority. The Supplier may also be expected to perform refresher training to The Authority, throughout the Contract Period at no extra charge.

The training provided shall be proportionate to the size and requirements of The Authority and will be specified by The Authority.

The Supplier shall ensure that all guidance and/or training documents are kept up to date, readily available to download online, available as hard copy upon request and are provided at no extra charge to The Authority.

The Supplier shall provide training with accessibility support for The Authority, in line with the Equality Act 2010.

Any required training and/or materials for Authority accessible portals/interfaces must be provided by The Supplier. Suppliers should indicate in their response if there are any additional costs for this. Details of portal requirements are covered under Sections 6.7 (Instruction Amendments & Cancellations) and 6.12 (End User Enquires).

The Supplier shall ensure that all staff involved in processing of Authority’s data must receive Information Security Training upon induction and annually thereafter as a minimum.

Suppliers must have in place within their organisation a published fraud response plan which clearly sets out its anti-fraud policy, including fraud reporting and anti-fraud and corruption training.

12. Documentation

Management Information & Reporting:
Details of required MI & reports are covered in the following sections:

- 6.14 (Financial Reconciliation)
- 6.13 (Reporting)
- 4.1 General Scope of the Service
- 10 (Management and Contract Administration)

The Authority’s invoicing procedures are detailed below:

All invoices and/or credit notes must be an original document. The Supplier to send an email to alert The Authority that the invoice is ready to download and be reconciled. This will allow The Authority to identify any potential issues early.

Any correspondence/enquiries which are sent to the designated email address for invoices/credit notes and are not an original invoice and/or credit note will be deleted, with no action being taken.

All invoices and/or credit notes will either need to be sent electronically as an attachment to an email or as a hard copy document through the post to the designated email or postal address listed below:

Email: ssa.invoice@sharedservicesarvato.co.uk
Postal Address: Shared Services Arvato
5 Sandringham Park
Swansea Vale
SA7 0EA

If an original invoice and/or credit note is sent electronically, then the same document **must not** be sent as a hard copy through the post and vice versa.

All electronics invoice and/or credit notes **must** be sent in a PDF format. Any documents which are received and are not in a PDF format will be deleted with no action being taken.

All invoices or credit notes must quote a valid Purchase Order number i.e. one that is in the format 8000XXXXXX. This will be found on the Purchase Order you receive.

A 10Mb maximum file size per email is applicable.

If the e-invoice is encrypted, this could result in the invoice being blocked by Arvato email security filters.

The e-invoices **must not** include profanities, as these will also be blocked by Arvato email security filters and may delay/stop the invoice being received.

You should not provide goods or services without receipt of a valid Purchase Order.

Do not undertake new work or supply goods or services in excess of the original Purchase Order Value.

If an incorrect Purchase Order number or no Purchase Order number is quoted the invoice will be returned to you. You will be able to handwrite the correct Purchase Order numbers on the invoices that are returned, however it is preferable that you change it on your system and reissue to ensure any future invoices are referenced correctly.

Credit notes should quote the Purchase Order number and your original invoice reference along with details of what the credit note applies to, particularly if it is not for the full value of the invoice.

Identify the business unit the invoice or credit note relates to e.g. The Authority.

Shared Services Arvato cannot be responsible for any e-invoice until it has been received. Responsibility for ensuring the e-invoice is received by Arvato in a timely manner lies with The Supplier.

All Supplier invoices and payment enquiries must be directed to Shared Services Arvato. If you contact the relevant business unit directly, they will direct you to Shared Services Arvato.

How to Notify us of a Change

If you change important information, such as your organisation's contact or bank details, we will need written official correspondence. Please notify Shared Services Arvato as soon as possible:

Shared Services Arvato
Tel: 0844 892 0343
Email: support@sharedservicesarvato.co.uk (Please do not email original invoices/credit notes to this email address)

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

Enquiring about progress of payments

For all payment and invoice queries you will need to contact the Shared Services Arvato Service and Support Desk directly on 0844 892 0343. When calling you should quote the Purchase Order number, your vendor account number (if known) and the business unit you are invoicing e.g. The Authority.

You should ask for your communication to be logged on a "service ticket" along with your contact details. This will allow all issues relating to your query to be logged under a unique reference number.

You should quote the service ticket number in any follow up conversations.

If Shared Services Arvato has the invoice but cannot release it for payment, you are required to take appropriate action to ensure it can be paid.

If the invoice has not been received by Shared Services Arvato, the responsibility is on you to get the invoice to Shared Services Arvato. If you are sending invoices to anyone other than Shared Services Arvato, please change your customer invoicing address to Shared Services Arvato.

If a response from Shared Services Arvato is required, one will be provided to you within 10 working days.

If you have any remittance queries, these should be discussed with Shared Services Arvato:

Tel: 0844 892 0343

Email: support@sharedservicesarvato.co.uk (Please do not email original invoices/credit notes to this email address)

You must also ensure that a statement is sent to Shared Services Arvato monthly to aid prompt payment of invoices (email and postal address as above).

All charges relating to the services provided will be invoiced on a calendar month basis in arrears to The Authority. Payments will be made against valid invoices within 30 days of receipt.

All invoices must be sent to the relevant address as instructed by each customer.

Invoices must clearly show the following: -

- Purchase Order number
- Vendor number
- Total Monthly Charges by MID/Chain listing
- Card charges
- Card Processing/Virtual card processing charges
- Other charges

Initial indications are that The Authority will require one consolidated invoice per month that will provide a summary of charges by Merchant ID/chain. In addition to the invoice, a monthly detailed statement providing management information by MID/chain is required in a format to be specified by each customer.

Suppliers are requested to submit a proposed invoice layout within the tender.

In the event that invoices are not sent to the stipulated address within the contract, the relevant customer shall not be held responsible for any loss or delay.

13. Arrangement for End of Contract

The existing Supplier shall fully cooperate with The Authority to ensure a fair and transparent re-tendering process for this contract. This may require The Supplier to demonstrate separation between teams occupied on the existing Contract and those involved in tendering for the replacement contract to prevent actual (or perceived) conflicts of interest arising.

This cooperation shall include payment of any refund or monies owed and shall include any material or information which needs to be returned to The Authority or handed over to a new Supplier (including arrangements for collating and sharing TUPE data). This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to The Supplier in the buying process.

At no additional cost to the Buyer, the Parties shall prepare and agree an Outline Exit Plan within 60 days of Start Date, which shall provide a high-level summary of the steps the Parties may be required to take to ensure continuity of service across a number of different exit scenarios. The Parties shall review the Outline Exit Plan when reasonably required and update the same.

The existing Supplier shall comply with any requirements/actions to assist in the migration of Customer/End User details or Data, to facilitate continuity of DD service(s) including but not limited to Automated renewal of DD Mandates, Sanctions/Blocked User Lists.

The Supplier will comply with all requirements for data retention or deletion as specified in the Data Processing Schedule included in the Invitation to Tender.

13.1 Potential Suppliers should note that the Transfer of Undertakings (Protection of Employment) Regulations 2006 (TUPE) may apply to their tender. Please see “Instructions for Tenderers” for more information.

13.2 The incumbent has indicated that TUPE is likely to apply in this case and must provide the relevant employee liability information for their personnel who are potentially in-scope of TUPE before contract commencement date.

13.3 The incumbent is aware of their legal obligation to pass Employee Liability Information to the successful tenderer and the associated timescales for doing so. The information shall be provided in the spreadsheet included in Annex 4.

14. Evaluation Criteria

Selection will be based on the Evaluation Criteria, encompassing the most economically advantageous tender, which demonstrates a high degree of overall value for money, competence, credibility and ability to deliver.

Your tender will be evaluated using the following weightings **and** the criteria weightings set out at Annex 1, to obtain the optimal balance of quality and cost.

Mandatory Requirements (if applicable)

Annex 1 provides details of any elements/criteria considered as critical to the requirement. These are criteria, which will be evaluated on a pass/fail basis. A failure may result in the tender being excluded from further evaluation.

Quality Criteria:

Annex 1 provides details of the quality criteria on which tenders will be evaluated. This will list the primary criteria along with the allocated percentage weighting and a description of the specific requirement. The overall percentage allocated for the Quality Criteria is outlined in the Table “Overall Weighting Allocation” and the method used to allocate scores is outlined below.

Quality Criteria Scoring Methodology:

The scoring methodology used to assess and allocate scores to each criteria are included in the table below.

Score	% of weighting awarded	Description
3	100	Fully meets/evidence provided that demonstrates the requirement can be met.
2	66	Minor concerns/issues that the requirement can be met.
1	33	Major concerns/issues that the requirement can be met.
0	0	Does not meet the requirement, not addressed or no evidence provided.

Based on the allocated score, a percentage will be calculated against each element using on the following calculation:

$$\frac{\text{(Allocated Score}}{\text{Maximum Score)}} \text{ X Weighting}$$

For example, “Quality Element 1” can be allocated a score between 0 and 100 but carries a weighting of 10%. Supplier A is given a score of 60 for this element so receives a score of (60/100 x 10) = 6%. The scores for each element will then be added together to calculate the overall Quality Criteria score.

Financial / Price Criteria

Evaluation of the prices submitted will be performed separately by a Commercial Finance Accountant and details will not be made available to the Quality Evaluation Panel. This is to ensure fairness and avoid any subconscious influence of a lower price on the quality scoring. The overall percentage weighting allocated for the Financial/Price Criteria is outlined in the Table “Overall Weighting Allocation”.

Financial / Price Criteria Scoring Methodology:

A Percentage Scoring Methodology will be used to evaluate all proposals for this requirement. This methodology is based on the following principles:
The lowest tendered price will be awarded the maximum score available. Each subsequent bid will be baselined to this score and will be awarded a percentage of the maximum score available. The calculation used is as follows:

$$\frac{\text{(Lowest Tendered Price}}{\text{Tender Price Submitted per Supplier)}} \text{ X Maximum Score Available (i.e. Weighting)}$$

For example, if the Financial/Price weighting allocation is 40%, the maximum score available is 40. Supplier A submits the lowest price of £100,000 and Supplier B submits a price of £180,000. Based on the above calculation Supplier A and B will receive the scores shown below:
Supplier A = 100k/100k x 40 = 40%

Supplier B = 100k/180k x 40 = 22.22%

Overall Weighting Allocation

Evaluation Criteria	Weighting
Quality Criteria at 50% and Social Value Criteria at 10%	**60%**
Financial / Price Criteria	**40%**
Total	**100%**

Calculation of Overall Score:

The allocated score for the Quality and Social Value Criteria (where applicable) will be added to the Financial/Price Factor score to calculate the overall score for each tender (out of a max available 100%). The tender with the highest overall score will be deemed as successful.

15. Points of Contact

Commercial Advisor	Name	**Redacted under FOIA section 40**
	Tel	**Redacted under FOIA section 40**
	e-mail	**Redacted under FOIA section 40**
	Address	Commercial Directorate DVLA Longview Road Swansea SA6 7JL
Project Lead/Business Area Contact Operations & Customer Service Directorate (OCSD)	Name	**Redacted under FOIA section 40**
	Tel	**Redacted under FOIA section 40**
	e-mail	**Redacted under FOIA section 40**

All queries/questions should be sent to the Commercial Advisor

16. Annexes:

Annex 1 – Evaluation Criteria:

Mandatory Criteria

Specifying Goods and / or Services

Mandatory Criteria	Mandatory Criteria Description	Pass/Fail
M1. General Requirements	Supplier is able to meet all MANDATORY requirements outlined in 6.1.	
M2. Direct Debit Creation Service	Supplier is able to meet all MANDATORY requirements outlined in 6.2.	
M3. Direct Debit Renewal Function	Supplier is able to meet all MANDATORY requirements outlined in 6.3.	
M4. Duplicate Payment Schedules	Supplier is able to meet all MANDATORY requirements outlined in 6.4.	
M5. Content of Correspondence	Supplier is able to meet all MANDATORY requirements outlined in 6.5.	
M6. Unsuccessful instruction set-up	Supplier is able to meet all MANDATORY requirements outlined in 6.6.	
M7. Instruction amendments and cancellations	Supplier is able to meet all MANDATORY requirements outlined in 6.7.	
M8. Collection Process	Supplier is able to meet all MANDATORY requirements outlined in 6.8.	
M9. Failed Collections	Supplier is able to meet all MANDATORY requirements outlined in 6.9.	
M10. Indemnity Claims	Supplier is able to meet all MANDATORY requirements outlined in 6.10.	
M.11 Complaints	Supplier is able to meet all MANDATORY requirements outlined in 6.11.	
M.12End User Enquiries	Supplier is able to meet all MANDATORY requirements outlined in 6.12.	
M13. Reporting	Supplier is able to meet all MANDATORY requirements outlined in 6.13.	
M14. Financial Reconciliation	Supplier is able to meet all MANDATORY requirements outlined in 6.14.	
M15. Interest on late receipt of Direct Debit funds	Supplier is able to meet all MANDATORY requirements outlined in 6.15.	
M16. Service Performance	Supplier is able to meet all MANDATORY requirements outlined in 6.16.1	
M17. Service Support	Supplier is able to meet all MANDATORY requirements outlined in 6.16.2	
M18. Incident Management	Supplier is able to meet all MANDATORY requirements outlined in 6.16.3	
M19. Change Management	Supplier is able to meet all MANDATORY requirements outlined in 6.16.4	
M20. Risk Management	Supplier is able to meet all MANDATORY requirements outlined in 6.16.5	

Mandatory Criteria	Mandatory Criteria Description	Pass/Fail
M21. Continuous Improvement	Supplier is able to meet all MANDATORY requirements outlined in 6.16.6	
M22. Service Management	Supplier is able to meet all MANDATORY requirements outlined in 6.16.7	
M23 Standards	Supplier is able to meet all MANDATORY requirements outlined in 6.16.8	
M24 Invoicing	Supplier is able to meet all MANDATORY requirements outlined in 6.16.10	
M25. Accreditations	Supplier must provide proof of their current accreditations where stipulated.	

Scored Quality Criteria

Primary Scored Criteria	Primary Scored Criteria Weighting (%)	Scored Sub-criteria Description	Individual Scored Sub - Criteria Weighting (%)
S1. Service Management Service Functionality	**22%**	S1.1 The Supplier must confirm that they are fully compliant with the current Direct Debit and Bacs Direct Credit Scheme Rules. Evidence or proof of accreditation or Standards must be provided. Details of the software solution to be provided, explaining whether the entire solution is BACS accredited. Please refer to requirements 6.1	2%
		S1.2 Provide a detailed submission on the overall solution proposed; how The Supplier will deliver all Services, Notifications, requested in line with Requirements Specification. This should include (but not be limited to): • The management of third parties, • Complying with data protection legislation (UK GDPR), • Initiating a Project Delivery Team and work collaboratively with The Authority; • How deadlines/timescales will be met for transition and Go Live; • Complying with defined industry standards • Managing future volumes/capacity in Transaction increases • Delivery of future service enhancements and improvements. Please refer to requirements 6.1 & 6.5	2%
		S1.3 Provide a detailed submission how the Direct Debit Creation and Renewal Services will operate, interact, provide and receive real-time/bulk responses; handle failures; supporting DVLA Customer Channels; securely capture Customer Data and where/how Hosted; enable/provide the functionality to request duplicate payment schedules. Supplier must outline how it will meet The Authority Requirements in collecting Vehicle Excise Duty for the 1st of the Month, depending on when the End User makes the application and Direct Debit request. Please refer to requirements 6.2 – 6.6 & 6.8 & 6.9	2%
		S1.4 Provide a detailed solution on how you will design/deliver functionality to 'Block' and prevent certain End Users from applying for a Direct Debit, based on a set criteria and eligibility rules, defined by The Authority. Including the migration of the existing register of 'Blocked' End Users from the incumbent Supplier's system. Please refer to requirements 6.2 – 6.6	2%
		S1.5 Provide detailed information and solution on how you will surface and provide functionality for The Authority agents to enquire, amend mandates; update name, postal address, email address and bank details, whilst retaining the same licensing	2%

		period and payment dates; how BACS automated updates will be actioned within 1 working day; Please refer to requirements 6.7	
		S1.6 Provide full details on how Cancellation Notifications will be processed, whether from Bank or The Authority, Individually and Bulk notifications; late notifications and End User Refunds; Authority Vehicle Registration Number Changes; Please refer to requirements 6.7	2%
		S1.7 Provide detailed information on how the collections and payments that are made via daily BACS files per bank account into a DVLA GBS (Government Banking Service) bank account will be managed and reconciled by The Supplier, taking in to account The Authority Volumes. Please refer to requirements 6.8 & 6.9	2%
		S1.8 Please outline how you will meet The Authority Requirements in handling collections that fail due to insufficient funds or other reasons and how they will be re-presented. Detail how MI reports will be provided and their content, providing example templates of data. Please refer to requirements 6.8 & 6.9	1%
		S1.9 Please provide full details of your Indemnity Claims process in line with the DD Guarantee including but not limited to: • how it will process Indemnity Claims and notify The Authority, ensuring prompt actions and enforcement action by The Authority; • how you will support The Authority in automatically Challenging Indemnities where appropriate; • how Indemnity funds will be reconciled by Supplier Please refer to requirements 6.10	2%
		S1.10 Demonstrate how you will support with transition, training and Technical support from a Helpdesk to: • Investigate issues (Technical, End User or Financial queries); • any user limitations; • how the system can be improved in line with Authority Agent experience and feedback; • a configurable criteria Search functionality; • Audit functionality and access traceability; including the integration of the 'Blocked User' list and relevant search facility of data, such as reason for addition; Please refer to requirements 6.12	2%
		S1.11 Provide an outline solution with the Technology and Software detail of how The Supplier will meet the Management Information and Reporting Requirements of The Authority. Detail how Management Information reports will be provided and their content, providing example templates of data. Please refer to requirements 6.13	1%
		S1.12 Supplier to provide full details of its Daily Financial Reconciliation function including but not be limited to:	2%

		• Roles and responsibilities • How this will be managed end to end. Ensuring reconciliation of the DVLA bank accounts and passing information to The Authority reconciliation team; notifying The Authority of failures in a timely manner; Providing daily/weekly/monthly reports to The Authority Finance Operations team; • Reporting of all Direct Debit Instruction Errors; assisting with reclamation of funds due to error; • Compensating The Authority for lost revenue due to Supplier error; • How you will support BACS or The Authority data fields changes if needed; • Maintaining accurate and auditable records; • The provision of Monthly reports by deadline. Please refer to requirements 6.14 & 6.15	
S2. Service and Support Requirements	**10%**	S2.1 Provide detail of your achieved and committed availability, capacity and responsiveness of your online Direct Debit creation service (production and test) and any customer self-service portal and detail of your performance (achieved and committed) of your mandate collections service (e.g. accuracy and timeliness). Please refer to Service Performance requirements 6.16.1	2%
		S2.2 Provide detail on your support model including details of helpdesk availability, methods of requesting support, prioritisation levels, definitions and response times, monitoring, any provision of a public status page and any functionality for customers to monitor online availability and BACS processing. Please refer to Service Support requirements 6.16.2	2%
		S2.3 Provide detail of your incident management process (for both service and security incidents) including identification, roles and responsibilities, communication plans, prioritisation levels, response and resolution targets, escalation process and reporting (root cause analysis, Major Incident Reports, customer accessible tools). Please refer to Incident Management requirements 6.16.3	1%
		S2.4 Provide detail of your change processes including: Frequency, level of service impact and communication plans for maintenance changes. Method for request, scope and deployment controls, assessment and approvals process for customer-initiated changes and Provision of any customer accessible test environments and their proximity to Production Please refer to Change Management requirements 6.16.4	2%
		S2.5 Provide details of your risk management process including identification, analysis, treatment, communication and collaboration with the customer. Please refer to Risk Management requirements 6.16.5	1%
		S2.6 Provide details of your CSI processes including identification, analysis, implementation and reporting. Please refer to Continuous Improvements requirements 6.16.6	1%

		S2.7 Provide details of your Service Management provision including roles & responsibilities, reporting frequency and scope/content. Please refer to Service management requirements 6.16.7	1%
S3. Business Continuity	**4%**	S3.1 Please provide business continuity and disaster recovery plans for this service detailing, but not limited to: • Physical and digital disruption • Resourcing • Disaster recovery • Testing of plans including frequency Please provide evidence of how you comply with the requirements of ISO22301 and provide up to date accreditation or equivalent.	4%
S4. Quality Assurance	**3%**	S4.1 Please demonstrate that you have an effective quality assurance system in place and demonstrate that meets ISO9001 or equivalent standards and provide evidence of up-to-date accreditation if held.	3%
S5. Sustainability	**3%**	S5.1 Please detail how you will meet the requirements laid out in Section 9.4, including providing your environmental policy.	3%
S6. Cyber Security	**4%**	S6.1 Please provide evidence of how you meet the requirements in Section 9.2 and provide evidence of Cyber Essentials (or CE+) accreditation.	4%
S7. Information Security	**4%**	S7.1 Please demonstrate how you adhere to the ISO27001 standards and provide evidence of up-to-date accreditation if held.	4%
S8. Social Value Outcomes	**10%**	S8.1 Please provide details of how you will ensure you meet the Tackle Workforce Inequality (Equal Opportunity) requirements outlined in Section 7.	10%
	Total = 60%		

Financial/Pricing Criteria

Primary Financial/Pricing Criteria	Financial/Pricing Weighting (%)	Description
Pricing Requirements	**40%**	**Refer to the Pricing Schedule**  Direct Debit STA - Pricing Schedule.xls:
	Total = 100%	

Annex 2 – Welsh Language Scheme Requirements

DVLA must ensure that arrangements and contracts with third parties that relate to the provision of services to the public in Wales are consistent with the terms of the Welsh Language Scheme and are implemented accordingly.

This means that where DVLA provides services in English through use of a 3rd party supplier, it will deliver the same quality of service to residents in Wales, specifically:

- documentation and publications in English and in Welsh will be provided to the same quality and timescale. The majority of forms and correspondence provided as part of the Service will be provided by DVLA.

- target times for response to correspondence will be the same whether the correspondence is conducted in English or in Welsh.

Where the service is supported by a corporate or telephone support service located outside Wales, it will not be practicable to offer a Welsh Language telephone service. However, The Supplier must offer those who call and who wish to speak in Welsh the option of writing in Welsh or continuing the conversation in English.

Suppliers must adopt a bilingual corporate identity within Wales. This means Welsh and English must be displayed on all material which displays corporate identity. This includes identity badges and vehicles.

All signs, which give information to the public, must be bilingual with the Welsh and English text being treated equally with regard to size, legibility and prominence.

Each agent or supplier who delivers services to the public on behalf of DVLA in Wales will be monitored on an annual basis to ensure compliance with the Welsh Language terms of their agreements or arrangements.

Annex 3 – DD Overview Service Model Diagram

Redacted under FOIA section 43(2)

Annex 4 – Employee Liability Information TUPE

Redacted under FOIA section 43(2)

Annex 5 – Procurement Counter Fraud Statement

The Driver and Vehicle Licensing Agency (DVLA) adopts a zero-tolerance approach to procurement fraud.

A counter fraud culture has been embedded at DVLA and is actively promoted amongst all staff, particularly procurement specialists.
DVLA is committed to continually improve the awareness and understanding of its staff to actively prevent, deter and detect procurement fraud.
DVLA expects the highest standards of conduct and integrity from its staff, potential suppliers and its contractors. Individuals and organisations have responsibilities in preventing, deterring and reporting any instances where procurement fraud is suspected or detected.
DVLA requires potential suppliers and its contractors to.

- act with integrity, propriety, honesty, objectivity, accountability and openness,
- take all reasonable steps, in accordance with Good Industry Practice, to prevent fraud by its staff and any sub-contractors,
- actively avoid, prevent and deter any behaviour or activity that might be considered as collusion, i.e., operating a cartel, bid rigging, bid suppression, cover bidding, bid rotation, market division and price fixing.
- actively avoid, prevent and deter any behaviour or activity that might be considered as bribery or corruption, in contravention of The Bribery Act 2010, e.g. paying a sum of money, or other inducement, directly or indirectly to any person/s in relation to any DVLA contract or tender for goods, works or services;
- declare any 'Conflict of Interest' that might arise before, during or after a procurement process,
- provide and maintain accurate contract performance records/data,
- provide and maintain accurate financial documentation, e.g. invoices,

DVLA requires its staff to;

- act with integrity, propriety, honesty, objectivity, accountability and openness,
- be alert to the possibility that unusual events or transactions could be indicators of procurement fraud,
- report details immediately through the appropriate channel if procurement fraud is suspected,
- Co-operate fully with the DVLA Counter Fraud & Intelligence Team.

In addition, DVLA requires its procurement specialists to;

- prevent, deter and detect procurement fraud,
- ensure adequate control measures exist and operate effectively,
- assess the risk of procurement fraud,

- regularly review and test control measures and implement new control measures where necessary.

We have a zero-tolerance approach to procurement fraud. If you identify or suspect procurement fraud, please contact us immediately on the following numbers:

DVLA Counter Fraud & Intelligence Team – 01792 782650
DVLA Whistle-blowing Hotline – 01792 788883k

If procurement fraud is identified or suspected, DVLA may:

- report the matter to the Police and share with Counter Fraud Organisations,
- disqualify a potential supplier from a procurement process,
- suspend or terminate a contract with a supplier,
- take steps to recover financial losses.